Universidad Autónoma de Madrid
Escuela politécnica superior

Grado en Ingeniería informática

Trabajo Fin de Grado

SEGURIDAD EN CLOUD PARA PYMES

Autor: David Muñoz Miranda
Tutor: Álvaro Ortigosa Juárez

JULIO 2017

SEGURIDAD EN CLOUD PARA PYMES

Autor: David Muñoz Miranda
Tutor: Álvaro Ortigosa Juárez

Grupo de la EPS: Grupo de Herramientas Interactivas Avanzadas (GHIA)
Dpto. de Ingeniería informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
JULIO 2017

Resumen

Resumen

El presente trabajo se ha enfocado en estudiar los aspectos de seguridad relacionados con la utilización de servicios en la nube (cloud computing), con énfasis en la problemática de las PyMEs. En primer lugar, se ha hecho un estudio de diversos problemas de seguridad informática a los que se enfrenta una PyME día a día, y las distintas soluciones tecnológicas ofrecidas por los proveedores de servicios cloud para minimizar esos peligros. En este contexto, se han elaborado una serie de manuales (explicaciones paso a paso) para guiar a un profesional no experto en el área en la implantación de estas tecnologías. El motivo es que en la mayoría de las ocasiones la documentación existente no cuenta con detalle todos los procedimientos, porque se presupone un nivel de conocimiento avanzado que muchas veces los profesionales no poseen, sobre todo si es la primera vez que utilizan dicha tecnología. Las tecnologías utilizadas se pueden encontrar en la tabla "Problemas generales". Estos manuales se han elaborado en base a la tecnología provista por un proveedor en concreto, Azure de Microsoft, elegido por las razones expuestas en el propio trabajo.

El segundo aspecto examinado ha sido el de los costes implicados en el uso de esta tecnología destinada a mejorar a seguridad. Como en el primer punto, el análisis se basa en la oferta de un proveedor en particular, por motivos de simplicidad y para poder ofrecer números concretos. Este análisis de costes se considera necesario porque no siempre quedan claros todos los cargos a los que haremos frente cuando utilizamos un producto. Por ejemplo, mientras creamos una máquina virtual se nos muestra el precio de tener encendida dicha máquina virtual, pero no se nos habla de los costes ocultos que trae consigo la utilización de dicha máquina virtual, como por ejemplo costes de almacenamiento y de uso de la red. Evidentemente esta información es sumamente útil a la hora de calcular los costes de utilizar tecnologías que mejoran la seguridad del sistema de las compañías.

Finalmente, no hay que olvidar que el uso de tecnología cloud introduce nuevos problemas de seguridad y privacidad. Por ello se analizan estos problemas y las medidas de protección que ofrecen los propios proveedores. Otra vez, el foco está en un proveedor de servicios, haciendo especial hincapié en los ataques de tipo DDOS. Aunque a priori pudiera parecer que los proveedores deben ofrecer protección ante este tipo de ataques, la realidad es esta protección, si existe, no es completa. Por este motivo, aquí se presentan soluciones alternativas a estos problemas, que pueden ser examinados en la tabla "Problemas en la nube".

Cuadro 1: Problemas generales

Problema	**Solución**
Administración del sistema y de los usuarios	Active Directory Azure Active Directory
Un usuario que tiene conexiones desde localizaciones no frecuentes	Acceso condicional
Autenticación en aplicaciones web o en cliente	Single Sign On
Seguimiento de posibles errores	Identity Protection
Infraestructura insegura	Azure Advisor
Filtrado de documentos	Azure Information protection
Almacenamiento de datos	Azure storage

Cuadro 2: Problemas de la nube

Problema	**Solución**	**En quien recae la solución**
Permisos a la hora de administrar todo el sistema	Separación de cuentas y autenticación en dos pasos	El usuario
Ataques a la nube	Diseño de la nube	La nube
Ataques de denegación de servicio	Firewall de nueva generación Aterta+ webhook	El usuario
Competencias de seguridad	Gestionar sólo lo que necesitemos	La nube

Palabras Clave

Seguridad, Computación en la nube para PyMEs, PyME, Azure, AWS, SaaS, IaaS, Paas, securizar, autenticar, DDOS.

Abstract

In this thesis three security aspects about the use of the cloud computing has been addressed, a special emphasis has been placed in studying the security aspects that may affect the SME companies. The first aspect, has been to examine different technologies that the cloud computing companies offers for protecting against the security risk that every SME will handle every day. Furthermore, in order to guide a non-expert professional in the process of adapt these technologies a serial of step by step guides has been written. Such guides have been created due to the existing documentation many times is not clear enough, and lack of small details that the professional who is facing for the very first time with these technologies will need. This happens because the existing documentation presuppose previous advanced knowledge. These technologies can be found on the table 'General problems'. These guides have been elaborated using the existing technology: ?Azure? from a cloud provider called ?Microsoft?, chosen for reasons explained in this thesis.

The second aspect has been about detailing the price of using the addressed technologies assigned to improve the security. As in the first point, this analysis has been done using the offer of a particular cloud provider, thanks to this, particular cyphers have been detailed. This is necessary because the documentation on the main pages of the cloud hosting may not be clear enough. For example, when a new virtual machine is being created with the selected provider, only the price of using the virtual machine is shown but, there are hidden costs, a price for using disk space and network must be paid.

Finally, the last chapter is about to understand the security risks that will appear when a company uses the cloud computing technologies. Due to this situation, these problems have been examined as well as how the companies that sell those technologies defend us against those risks. Again, the focus is on a special cloud provider. A special emphasis has been made on searching for protection against DDOS attacks like, as we will see, the cloud computing companies do not protect us against those attacks as they could. For this reason, alternative solutions have been presented and can be seen in the table 'Cloud Risk'.

Cuadro 3: General problems

Problem	**Azure Solution**
System and user management	Azure Active Directory Active Directory
An user connectects from untrusted locations	Conditional access
Authentication on web or client apps	Single Sign On
Error tracing	Identity Protection
Advices about security risk	Azure Advisor
Data leaks	Azure information protection
Data Storage	Azure Storage

Cuadro 4: Cloud Risks

Problem	**Solution**	**Who sould deal with the problem**
Permissions	Multi-factor authentication and permisssons delimitation	The user
Attacks to the cloud	Cloud Design	The cloud hosting
Distributed Denial of Service Attack	New generation firewall Alert + webhook	The user
Security Compliance	Manage what we need to	The cloud hosting

Key words

PYME, Azure, AWS, SaaS, IaaS, Paas, securify, authentication, DDOS.

Agradecimientos

A mi padre, allá donde quiera que esté por dármelo todo y a la vez no darme nada, siempre me diste los mejores consejos que podías darme, pese a que yo en muchas ocasiones no quisiera escucharlos. A mi madre, por darme su apoyo y por hacer parecer que los problemas son menos de lo que en realidad son. Gracias a vosotros soy quien soy.

A todos los amigos que he hecho durante la carrera, gracias a vosotros soy más maduro y más fuerte que cuando comencé la misma, soy mejor persona gracias a vosotros. Sobre todo tengo que agradeceros aguantarme los días que no he estado de buen humor, debido a que las cosas no me salían como yo quería, por servir de conejillos de indias de algún experimento de este trabajo y por escuchar los problemas que he tenido.

A todos mis amigos, gracias por estar ahí siempre, por darme vuestro apoyo y ayudarme a liberar la mente.

A Álvaro Ortigosa Juárez, mi tutor de este trabajo, gracias por sacar más tiempo del que en ocasiones tenías para aconsejarme, guiarme y sobre todo para decirme lo que estaba haciendo mal.

A Ricardo Martínez García, mi mentor en el programa IMP. Gracias por todos los consejos que me has dado para afrontar mi futuro.

Índice general

Índice de Figuras

Índice de Tablas

1 Introducción

1.1. Motivación del proyecto

A mediados del siglo XX, aunque en la actualidad no haya sido reconocida oficialmente, comenzó sin lugar a dudas la revolución informática y con ella una época en la manera de realizar todo tipo de tareas ha cambiado drásticamente una y otra vez, pese a que no hayamos querido, nos hemos tenido que adaptar a ésta revolución y aplicarla en nuestro día a día. Como ejemplo de estos cambios podemos observar tres situaciones:

La primera de ellas la aparición de los ordenadores personales. Gracias a Steve Jobs y Bill Gates, hoy en día prácticamente en todos los hogares de los países desarrollados podemos encontrar uno o más ordenadores ¿Para qué quiero yo un cacharro de esos en casa? Seguramente es una frase que mis progenitores dijeron más de una vez, al igual que los lectores más jóvenes o incluso usted. Si está en el último grupo y tiene hijos de cierta edad seguro que dispone de un ordenador al igual que sus hijos, esto es porque la herramienta ha evolucionado y no sólo tiene un fin como pueda ser el trabajo, hoy en día un ordenador tiene fines laborales, lúdicos, sociales...

El segundo ejemplo lo podemos observar en los teléfonos móviles. Cuando yo era un adolescente recuerdo mi primer dispositivo móvil, un Siemens A50, con este tipo de dispositivos se podía llamar, enviar y recibir mensajes y poco más. Cuando empezaron a introducir móviles que se conectaban a Internet (antes de los Smartphones), recuerdo haber pronunciado la frase ¿Para qué quiero yo Internet en el móvil? Actualmente carecer de Internet es dejar de disponer de infinidad de aplicaciones que usamos cada día.

Aunque la situación que nos concierne es la nube (*Cloud* para los angloparlantes). Desde hace bastantes años, las empresas han usado servidores para almacenar sus aplicaciones, datos y básicamente todos los activos digitales de la compañía. Había empresas que alquilaban servidores a otras compañías (como Telefónica) para que dispusiesen de dichos servidores en sus instalaciones, ahorrando a la contratante un espacio y ciertas tareas de mantenimiento. Ese fue el nacimiento de la nube, hacer uso de hardware del que no disponemos. Hoy en día la nube nos rodea, está por todas partes, pero muchos usuarios a la vez que muchos informáticos no tienen bien claro lo que es. ¿Para qué voy a usar yo la nube? se preguntará algún administrador de sistemas. Pues eso es lo que se ha investigado en este trabajo, los beneficios que tiene el uso de dicho este nuevo concepto en las empresas en el ámbito de la seguridad así como los problemas

que puede aparecer al hacer uso de dicha tecnología.

1.2. Objetivos y enfoque

Las grandes entidades disponen normalmente de varias personas encargadas de los equipos informáticos de las mismas, incluso las muy grandes disponen de varios equipos de personas que se encargan de llevar a cabo tareas concretas. Sin embargo existen muchas compañías que no pueden disponer de tal lujo debido a que su plantilla es muy limitada, estoy hablando de las pequeñas y medianas empresas, aquellas que cuentan con menos de doscientos cincuenta empleados, a dichas empresas se las conoce como PyMEs.

En España la gran mayoría de ellas son pequeñas, es decir tienen menos de diez empleados [1], lo que significa que no pueden dedicar demasiados recursos a proteger los sistemas informáticos de los que dispongan, ya sea una página web, una base de datos o algún recurso de almacenamiento y ver comprometida la información que una empresa posee puede traer inconvenientes muy serios. Además, hay que tener en cuenta que aproximadamente tres cuartas partes de las empresas españolas poseen un sitio web, y son muchas las que tienen que mejorar la seguridad de su entorno.

No hace falta ser una empresa excesivamente muy grande para ver cómo la pérdida de la información afecta a la compañía: imagine que la empresa guarda en una hoja de cálculo clientes con los que se comercia y la cantidad a la que se le vende los productos. Si dicha hoja de cálculo cae en manos de la competencia, pueden llamar a nuestros clientes y ofrecerle los mismos servicios un poco más baratos, sería la ruina de la empresa. Otro escenario posible es que la compañía se dedique al comercio electrónico a pequeña escala a través de una página web, si sube los precios de nuestros productos hasta que se descubra lo que está pasando se obtendrían perdidas. Asimismo, si ese atacante consigue los datos de los clientes la empresa habría concurrido en delito al haber vulnerado la Ley Orgánica de Protección de Datos que ha de ofrecer a sus clientes. Ante estas situaciones se abren dos posibilidades: la primera y seguramente más común sea subcontratar a una empresa que nos lleve los sistemas informáticos y se haga responsable de la seguridad de los mismos; la segunda posibilidad será utilizar lo que se denomina computación en la nube, lo cual nos abre un entorno de trabajo en el que podremos albergar dichos sistemas aumentando en cierto modo la seguridad de una manera sencilla. Éste último caso será el que se verá tratado en el presente escrito: a través de uno de los múltiples proveedores en la nube existentes, se realizarán desde un punto de vista de la seguridad una serie de guías para aumentar la seguridad en los sistemas informáticos de una pequeña o mediana empresa.

1.3. Metodología y plan de trabajo

Para realizar este trabajo, se ha hecho uso de la plataforma en la nube que pone a disposición Microsoft cuyo nombre es Azure. La razón por la que se ha decidido hacer uso de dicha plataforma es que se dispone de varias cuentas con cierto crédito mensual, dicho recurso no se ha obtenido en otras plataformas, ya que ofrecen cuentas de prueba pero el créditos que estas proveen no hubiera alcanzado para cumplimentar la magnitud de este trabajo. Cabe destacar que todas las plataformas con servicios disponibles en la nube tienen como objetivo mejorar la seguridad de los sistemas que albergan y que algunas son compatibles entre ellas, por ejemplo, la nube de Amazon ofrece un servicio de la plataforma Microsoft llamado Active Directory lo que facilita tener parte de la infraestructura con otro proveedor.

Para elaborar este trabajo se ha decidido hacer una división en tres partes. En la primera parte, se explicará cómo el proveedor pone a disposición del usuario ciertos servicios para mejorar

la seguridad del sistema hospedado. Cada vez que se explique un servicio nuevo se detallará paso a paso cómo se instala y configura en la plataforma de Azure así como una explicación de en qué consiste dicho servicio; en la segunda parte, se detallará el precio de utilizar las tecnologías vistas en el primer apartado. Finalmente, en la tercera parte, se abordarán riesgos de seguridad presentes cuando se ubica un servicio en la nube y cómo el servicio que hemos elegido para este trabajo los aborda.

1.4. Otras tecnologías

Como se ha comentado previamente, la nube que he utilizado para los experimentos es la de Azure, pero existen otras muchas, tales como Amazon Web Services, Google Cloud, IBM, DigitalOcean u Oracle Cloud. En cuanto a usuarios, la de Amazon tiene el cincuenta y cinco por siento de la cuota de mercado por un veinticinco por cierto de la de Azure en segundo lugar y Google Cloud con un quince por ciento en tercera posición. Las dos últimas nombradas son las que más usuarios han ganado en el presente año y se espera que sigan creciendo y arrebatándole cuota a Amazon [2]. Aún tratando muchas tecnologías a la hora de hacer nuestro entorno más seguro en este trabajo, cabe destacar que la nubes de la competencia también tienen tecnologías que sirven para el mismo propósito en la mayoría de casos como se detalla en la siguiente tabla [3] [4] [5].

Cuadro 1.1: Comparativa de tecnologías

Tecnología	**Tecnología en Microsoft Azure**	**Tecnología en Amazon Web Services**	**Tecnología en Google Cloud**
Tienda de servicios	Azure Marketplace	AWS Marketplace	No disponible
Máquinas virtuales	Azure Virtual Machines	Elastic Compute Cloud VM	Compute engine
Almacenamiento	Azure Storage	Simple storage services	Cloud Storage
Tutor en la nube	Azure Advisor	Trusted Advisor	Google Cloud Platform Security
Portal Web	Portal de Azure	CloudWatch	StackDriver
Gestor de almacenamiento	Azure storage explorer	Herramientas de terceros	No disponible
Autenticación de usuarios internos	Azure Active Directory	Identity and access management	Cloud IAM
Autenticación de usuarios externos	Azure Active Directory B2C	No encontrado	No encontrado
Autenticación en dos pasos	Multi-Factor Authentication	Multi-Factor Authentication	No encontrado
Protección al sacar los datos	Azure Information Protection	No encontrado	No encontrado
Seguridad automatizada	Security center	Inspector	No encontrado

2

Soluciones ofrecidas por la nube

2.1. Introducción

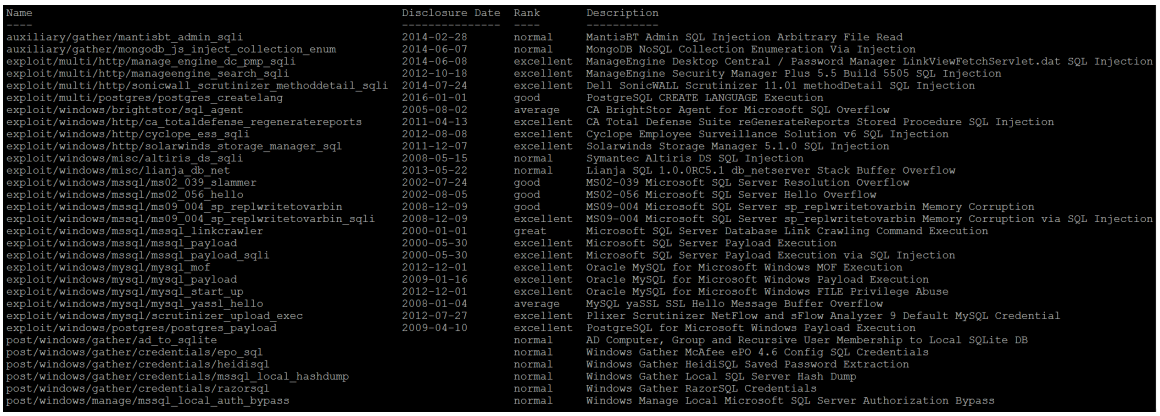
La primera vez que asistí a una charla sobre seguridad hace ya siete años, el ponente empezó diciendo que la seguridad total no existe, y en sucesivas lecturas no he parado de encontrarme con esta postura. Podemos conseguir sistemas muy seguros, pero no podremos tener la seguridad total de que no existe ningún punto de fallo en el mismo. Esto puede resultar chocante para una persona que no tenga demasiados conocimientos en informática, pero es un hecho, el único sistema seguro es aquel que no existe. Pongamos que tenemos un disco duro con la fórmula de la vida eterna, como consideramos que esta información es demasiado peligrosa para que salga a la luz, pero que no queremos destruir la información, de tal manera decidimos construir un búnker a 10 KM de profundidad, dentro construimos una sala con puertas de acero blindadas y en su interior colocamos nuestro disco duro. A continuación, cerramos las puertas, sellamos los accesos con hormigón y fundimos todas las llaves. ¿Podemos decir con total seguridad que nadie nunca jamás conseguirá entrar en la sala y hacerse con el disco duro? La respuesta es no (Seguro que al lector se le ocurren maneras imaginativas para hacerse con el disco duro), aunque podemos decir sin embargo que dicho sistema es muy seguro y que el atacante tendrá que esforzarse mucho para conseguir hacerse con el control del sistema. Con la seguridad informática pasa algo semejante, no podemos garantizar la seguridad total del sistema.

Una PyME por definición tendrá menos de 250 trabajadores por lo que no siempre podrá disponer de un equipo dedicado a la seguridad de la infraestructura de la empresa, en numerosas ocasiones dispondrá de apenas uno o dos informáticos que serán los encargados de la gestión de los equipos informáticos de la empresa. Esto puede resultar algo chocante ya que, hoy en día aparecen más y más tecnologías y las empresas hacen uso de ellas, el uso de más tecnologías como consecuencia trae la aparición de más y más riesgos en la seguridad.

Una página web podrá sufrir ataques SQL, XSS, Broken Authentification y un gran número de ataques distintos. La compañía *owasp* ha creado una lista de los 10 ataques más comunes a una página web y ciertas recomendaciones sobre cómo intentar evitarlos o mitigarlos, para ello podemos acceder a su página web `https://www.owasp.org`

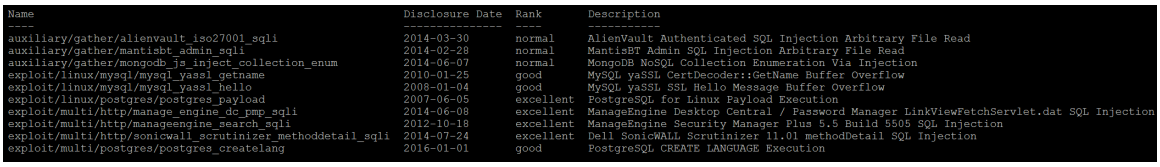
A su vez una compañía dispondrá de una base de datos en un servidor, existiendo un gran número de ataques contra los diversos tipos de servidores existentes tal y como podemos ver en

la siguiente imagen, realizando búsquedas sobre SQL en equipos Windows Y Linux (Figuras: Exploits SQL Windows, Exploits SQL Linux).



Name	Disclosure Date	Rank	Description
auxiliary/gather/mantisbt_admin_sqli	2014-02-28	normal	MantisBT Admin SQL Injection Arbitrary File Read
auxiliary/gather/mongodb_js_inject_collection_enum	2014-06-07	normal	MongoDB NoSQL Collection Enumeration Via Injection
exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
exploit/multi/http/manageengine_search_sqli	2012-10-18	excellent	ManageEngine Security Manager Plus 5.5 Build 5505 SQL Injection
exploit/multi/http/sonicwall_scrutinizer_methoddetail_sqli	2014-07-24	excellent	Dell SonicWALL Scrutinizer 11.01 methodDetail SQL Injection
exploit/multi/postgres/postgres_createlang	2016-01-01	good	PostgreSQL CREATE LANGUAGE Execution
exploit/windows/brightstor/sql_agent	2005-08-02	average	CA BrightStor Agent for Microsoft SQL Overflow
exploit/windows/http/ca_totaldefense_regeneratereports	2011-04-13	excellent	CA Total Defense Suite reGenerateReports Stored Procedure SQL Injection
exploit/windows/http/cyclope_ess_sqli	2012-08-08	excellent	Cyclope Employee Surveillance Solution v6 SQL Injection
exploit/windows/http/solarwinds_storage_manager_sql	2011-12-07	excellent	Solarwinds Storage Manager 5.1.0 SQL Injection
exploit/windows/misc/altiris_ds_sqli	2008-05-15	normal	Symantec Altiris DS SQL Injection
exploit/windows/misc/lianja_db_net	2013-05-22	normal	Lianja SQL 1.0.0RC5.1 db_netserver Stack Buffer Overflow
exploit/windows/mssql/ms02_039_slammer	2002-07-24	good	MS02-039 Microsoft SQL Server Resolution Overflow
exploit/windows/mssql/ms02_056_hello	2002-08-05	good	MS02-056 Microsoft SQL Server Hello Overflow
exploit/windows/mssql/ms09_004_sp_replwritetovarbin	2008-12-09	good	MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption
exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sqli	2008-12-09	excellent	MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Injection
exploit/windows/mssql/mssql_linkcrawler	2000-01-01	great	Microsoft SQL Server Database Link Crawling Command Execution
exploit/windows/mssql/mssql_payload	2000-05-30	excellent	Microsoft SQL Server Payload Execution
exploit/windows/mssql/mssql_payload_sqli	2000-05-30	excellent	Microsoft SQL Server Payload Execution via SQL Injection
exploit/windows/mysql/mysql_mof	2012-12-01	excellent	Oracle MySQL for Microsoft Windows MOF Execution
exploit/windows/mysql/mysql_payload	2009-01-16	excellent	Oracle MySQL for Microsoft Windows Payload Execution
exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	Oracle MySQL for Microsoft Windows FILE Privilege Abuse
exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	MySQL yaSSL SSL Hello Message Buffer Overflow
exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
exploit/windows/postgres/postgres_payload	2009-04-10	excellent	PostgreSQL for Microsoft Windows Payload Execution
post/windows/gather/ad_to_sqlite		normal	AD Computer, Group and Recursive User Membership to Local SQLite DB
post/windows/gather/credentials/epo_sql		normal	Windows Gather McAfee ePO 4.6 Config SQL Credentials
post/windows/gather/credentials/heidisql		normal	Windows Gather HeidiSQL Saved Password Extraction
post/windows/gather/credentials/mssql_local_hashdump		normal	Windows Gather Local SQL Server Hash Dump
post/windows/gather/credentials/razorsql		normal	Windows Gather RazorSQL Credentials
post/windows/manage/mssql_local_auth_bypass		normal	Windows Manage Local Microsoft SQL Server Authorization Bypass

Figura 2.1: Exploits SQL Windows



Name	Disclosure Date	Rank	Description
auxiliary/gather/alienvault_iso27001_sqli	2014-03-30	normal	AlienVault Authenticated SQL Injection Arbitrary File Read
auxiliary/gather/mantisbt_admin_sqli	2014-02-28	normal	MantisBT Admin SQL Injection Arbitrary File Read
auxiliary/gather/mongodb_js_inject_collection_enum	2014-06-07	normal	MongoDB NoSQL Collection Enumeration Via Injection
exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	MySQL yaSSL CertDecoder::GetName Buffer Overflow
exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	MySQL yaSSL SSL Hello Message Buffer Overflow
exploit/linux/postgres/postgres_payload	2007-06-05	excellent	PostgreSQL for Linux Payload Execution
exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
exploit/multi/http/manageengine_search_sqli	2012-10-18	excellent	ManageEngine Security Manager Plus 5.5 Build 5505 SQL Injection
exploit/multi/http/sonicwall_scrutinizer_methoddetail_sqli	2014-07-24	excellent	Dell SonicWALL Scrutinizer 11.01 methodDetail SQL Injection
exploit/multi/postgres/postgres_createlang	2016-01-01	good	PostgreSQL CREATE LANGUAGE Execution

Figura 2.2: Exploits SQL Linux

Además, las compañías que dispongan de más de 20 ordenadores suelen disponer de un servicio LDAP para la administración de los usuarios, permisos y toda la infraestructura de la empresa ya que se estima que con ese número de empleados comienza a ser recomendable la instalación de un servicio LDAP para la administración. Este servicio suele ser una fuente de vulnerabilidades y es grave que se encuentre una vulnerabilidad en dicho servicio, dado que mediante un escalado de servicios el atacante podrá obtener acceso a cualquier bien informático de la empresa.

Pero: ¿Son las aplicaciones los únicos puntos de exposición? La respuesta es no. Bien es conocido que las redes Wifi no brillan por su seguridad sobre todo si no dedicamos demasiado esfuerzo en hacerlas más seguras, lo que puede ocurrir en empresas cuyo departamento informático no sea muy amplio. Otro punto en el que los atacantes pueden poner su foco es en las personas, un empleado puede publicar información en las redes sociales que ayuden a un atacante a encontrar información para conseguir entrar a nuestro sistema.

Estos son demasiados riesgos a tener en cuenta para un departamento como los que estamos considerando sin demasiados recursos. De tal manera lo mejor que puede ocurrir es que se tengan que preocupar del menor número de puntos de ataque posible. En esta sección veremos los puntos en los que el simple hecho de migrar nuestro sistema a Azure conseguirá hacer más seguros los sistemas de la empresa. Esto no quiere decir que el riesgo de seguridad desaparezca por completo como hemos dicho anteriormente.

2.2. Responsabilidades

En esta sección veremos los riesgos que podría tener nuestro sistema, los cuales delegaremos o desaparecerán por el mero hecho de portar el sistema o parte de él a Azure.

En primer lugar pasamos a analizar los puntos de manera simplificada de los que debemos preocuparnos al utilizar SaaS, PaaS, IaaS o servidores físicos `https://aka.ms/securecustomer`.

En la Figura: Responsabilidad de seguridad que mejor define de qué se debe encargar el usuario cuando usa servicios en la nube, sea del proveedor que sea, intentemos desglosarla paso por paso:

- Parte física...
  - En servidores On Premise, el administrador será el encargado del equipo físico en el que servidor será hospedado conocerá la marca del Hardware y será el encargado de garantizar su disponibilidad.
  - Al usar cualquier servicio en la nube, el administrador desconocerá todo lo que tenga que ver a nivel de Hardware, no conocerá.
- Sistema operativo ...
  - Tanto en equipos On premise como en Iaas el administrador será en encargado de gestionar el sistema operativo en el que se alojarán los servicios prestado. El administrador será el encargado de actualizar las aplicaciones aplicando parches de seguridad cuando sea necesario.
  - Tanto en SaaS como en PaaS el host en la nube se encargará de todo lo relacionado con el sistema operativo.
- Controles de red y aplicación....
  - Tanto en Paas, IaaS y On premise el administrador deberá controlar la aplicación internamente, un ejemplo puede ser una página web codificada al 100 % por la compañía.
  - En SaaS el administrador únicamente gestiona la aplicación pero no la controla.
- Control de acceso
  - En todos escenario será el administrador el que se encargue de gestionar cómo hacen uso los usuarios del sistema y de los permisos que puedan tener.

Todo esto no representa que desaparezcan riesgos de seguridad al migrar parte el total de nuestra plataforma a la nube, pero representa no seremos nosotros los que debemos gestionar este área. Esto puede mejorar dos aspectos muy importantes para la empresa, el primero de ellos la disponibilidad, los proveedores en la nube se comprometen a dar alta disponibilidad en sus servicios de pago, por ejemplo Azure se compromete a que nuestros servicios estarán disponibles en un 99'5 % del tiempo como mínimo `https://azure.microsoft.com/es-es/support/legal/sla/summary/`. El segundo aspecto es la seguridad, una empresa que no disponga de una sección altamente dedicada no podrá hacer frente a todos los aspectos de seguridad a los que si puede una compañía más grande. Si la compañía va a alojar un servicio web, utilizando PaaS dejará de preocuparse de los riesgos de seguridad que pueda tener el sistema operativo en el que se ve alojado, así como de problemas en el hardware que puedan surgir.

2.3. Active Directory y Azure Active Directory

Figura 2.3: Responsabilidad de seguridad

2.3.1. Active Directory

En toda compañía en la que sus usuarios utilicen equipos informáticos los usuarios están utilizando como mínimo dos recursos, el primero de ellos su usuario y contraseña y en segundo lugar un equipo informático con un sistema operativo. Si usted tiene un único ordenador en casa la administración de los usuarios y la administración del equipo la realiza de forma local, es decir cualquier tema de administración del equipo la lleva a cabo sobre el mismo equipo y para realizar dicha tarea debe tener contacto físico con dicho ordenador. En una empresa cuando hay pocos equipos y usuarios esta tarea es posible llevarla a cabo, pero cuando llegamos a cierta cifra necesitamos que esa administración no sea de forma local, sino que se lleve a cabo por la persona que administra los equipos de manera descentralizada y automática, lo que permite que si queremos una tarea sobre ciertos equipos realizarla una única vez y que esa acción se aplique a los equipos deseados. Además, sería conveniente tener un servidor central que sea el encargado de permitir la autenticación de los usuarios sobre sus equipos, lo cual nos permitiría que con cada nueva incorporación a la compañía se crease el usuario en dicho servidor, para que fuese capaz de utilizar las credenciales de acceso en los equipos de la compañía. Con dicha finalidad se creó el protocolo LDAP, un protocolo que pueden utilizar tanto equipos Windows como Linux o MAC.

Los servidores más tradicionales para la implementación de estos servicios son Bind9 en entornos Linux y Active Directory en entornos Microsoft, estos servidores nos permiten crear un dominio bajo el que se englobaría los recursos que queremos administrar. No es competencia de este trabajo explicar más a fondo las funcionalidades de este servicio, sobre todo teniendo

en cuenta que la mayoría del público al que va dirigido este trabajo representa compañías de menos de diez personas una cantidad insuficiente para implementar dicho servicio, pero con unos veinte o treinta usuarios equipos en la compañía ya sería suficiente para su implementación, como seguramente las compañías con una cantidad superior a esa cifra ya tengan instalado el servicio o tengan planeada su implementación, vamos a hablar un poco sobre las opciones que nos ofrecen plataformas en la nube para implementarlo.

En primer lugar, AWS nos ofrece dos servicios [6], el primero de ellos AWS Directory Service es compatible totalmente con entornos Linux, Microsoft y MAC y nos ofrece muchas de las funcionalidades que ofrece Active Directory. El segundo servicio que nos propone se trata de Active Directory y nos permite ejecutar las mismas acciones que éste, ya que instala una máquina virtual con el servicio de Active Directory instalado.

En segundo lugar la nube de Microsoft, Azure no nos ofrece Active Directory como tal, nos ofrece un servicio denominado Azure Active Directory (AAD) que poco tiene que ver, del que hablaremos más adelante. Por lo que si queremos instalar un servidor de Active Directory deberemos de hacerlo sobre una máquina virtual, tal y como se cuenta al comienzo de la sección 'primer escenario', en el caso de que ya dispongamos de un servidor físico y queramos subirlo como máquina virtual a Azure también podemos efectuar dicha acción tal. Como hemos visto en la sección de 'Responsabilidades' de este mismo capítulo montar un servidor sobre una máquina virtual en lugar de en una máquina física, puede ayudar a mejorar la seguridad.

2.3.2. Azure Active Directory

Aunque esta tecnología comparta apellidos con la vista en la sección anterior y tenga ciertas similitudes, sirve para objetivos diferenciados, si bien Active Directory nos permite administrar usuarios, equipos y permisos AAD nos sirve para administrar usuarios y sus permisos de acceso, pero en lugar de permitir el acceso a un equipo como hace Active Directory, nos permite el acceso a aplicaciones, ya sean aplicaciones de escritorio tradicionales o aplicaciones web, dando igual donde estén alojadas las mismas, si en Azure, AWS o un servidor on premise. Este servicio será esencial en posteriores apartados y tiene varias ventajas, para empezar que este es un servicio Saas, por lo que la seguridad de la infraestructura queda para Microsoft, nosotros simplemente en cuanto a este apartado se refiere nos tenemos que preocupar de las credenciales de acceso de los usuarios no se filtren. En segundo lugar es que este servicio es muy difícil que deje de prestar servicio por una caida de un servidor, ya que toda la información se replica a todos los centros de Azure por lo que aunque el más cercano no se encuentre operativo otro nos dará el servicio [7]. La última de las ventajas, aunque se tratará en el tema de costes es que en su versión más básica es un servicio gratuito y podemos autenticarnos contra todas las aplicaciones que quedamos.

2.4. Autenticación en web y apps

En esta sección se verá cómo hacer uso de la autenticación que nos provee Azure mejorará sin mucho esfuerzo la seguridad a la hora de autenticar usuarios en nuestras páginas Web.

Cuando queremos desarrollar una App tenemos que pensar en dos aspectos, el primero de ellos la manera en la que vamos a almacenar los usuarios, y el segundo la manera en la que los usuarios se van a autenticar contra el sistema. Ambos aspectos conllevan riesgos de seguridad que son un quebradero de cabeza para cualquier desarrollador y mucho más para una persona que no sea un experto programador. Las maneras de guardar los datos de los usuarios son múltiples con sus respectivos riesgos, la más rudimentaria pasaría por guardar estos datos en un fichero plano y recorrer todo el archivo con un bucle 'for' cada vez que un usuario se intente autenticar

contra el sistema, evidentemente esto es poco práctico, muy costoso y muy inseguro. Otra manera sería guardar los datos de los usuarios en una base de datos, esto hace que las búsquedas sean más rápidas y añade seguridad. A este entorno con una base de datos podemos añadir muchas capas de seguridad, pero a no ser que dediquemos mucho tiempo a esta tarea, siempre quedarán resquicios que alguien malintencionado pueda aprovechar para burlar la seguridad. El segundo aspecto del que nos debemos preocupar es cómo se autentican los usuarios, viene a ser la manera en la que el equipo cliente envía la información al servidor y la manera en la que éste responde. Podemos enviar todas las comunicaciones sin encriptar, pero con un 'sniffer de red' podemos ver el tráfico que envía el cliente al servidor y viceversa. Ésta práctica es muy insegura y por ello se usan muchos tipos de cifrados, cuando vemos el icono del candado en nuestro navegador significa que nuestras comunicaciones están protegidas por algún tipo de encriptación.

2.4.1. Autenticación contra usuarios de AAD

Tanto usar una base de datos y añadirles seguridad como encriptar las comunicaciones son muy buenas prácticas para la autenticación, pero ambas llevan tiempo si se quieren llevar a cabo de la mejor manera posible. Lo que nos ofrece Azure para solucionar estos dos aspectos es usar como base de datos 'Azure Active Directory' y como método de autenticación 'Single Sign on' (SSO) [8]. Azure Active Directory como se ha comentado previamente es una plataforma SaaS y, SSO es un método de autenticación. Tradicionalmente cuando queremos autenticarnos contra un servidor es a ese servidor al que le enviamos las credenciales de acceso y con ellas decide si nos lo otorga o no, además cada vez que necesitamos autenticarnos en un sitio web necesitamos introducir nuestras credenciales. SSO funciona de manera diferente, en lugar de autenticarnos contra el recurso que queremos utilizar nos autenticamos contra un servidor de credenciales de Microsoft, delegando toda la seguridad de la autenticación en dicho servidor, si la autenticación es exitosa, nos devolverá un tokem que se guardará temporalmente en nuestro equipo y, cuando queramos autenticarnos contra un recurso, automáticamente el recurso cogerá el tokem y nos dará acceso, por lo que no hace falta que estemos introduciendo nuestras credenciales cada vez que queramos autenticarnos contra una aplicación.

Azure nos ofrece la posibilidad de utilizar su servicio con las aplicaciones de su tienda o las que nosotros desarrollemos utilizando ASP, en esta sección lo utilizaremos para autenticarnos en páginas web, pero puede utilizarse para autenticación en aplicaciones en la nube (Docker) o incluso aplicaciones locales de nuestros equipos. El listado de aplicaciones que se puede utilizar se encuentra en `https://azuremarketplace.microsoft.com/es-ES/marketplace/apps`. Una muy interesante para las empresas es Wordpress, ya que pueden tener un blog para sus usuarios, también hay aplicaciones como dropbox realmente útiles.

En el anexo del segundo escenario podemos ver cómo crear una aplicación ASP y otra aplicación con Wordpress utilizando esta tecnología. Aunque el problema de utilizar AAD para autenticar a nuestros usuarios es que debemos de darles de alta manualmente en ADD, no tendríamos una página web en la que los usuarios se pudiesen registrar.

Una de las ventajas más importantes que nos ofrece Single Sign On, es que un usuario sólo tendrá un nombre de usuario y contraseña para acceder a cualquier sistema que implemente la tecnología para la organización y, si se ha autenticado en una web usando dicho usuario, no necesita volver a autenticarse en otra aplicación si utiliza la misma sesión en el explorador web (No cierra y abre el navegador web). Aunque esto puede verse como un problema, debido a que, si el usuario ve su contraseña comprometida, verá comprometidas todas las aplicaciones en las que usuario tiene acceso.

2.4.2. Autenticación con Azure Active Directory B2C

En la subsección anterior nos ha surgido un problema, la seguridad de las aplicaciones está en manos de Azure, pero los usuarios tienen que estar registrados por nosotros en nuestro AAD ya sea a mano o programando un apartado de registro en el cual usaríamos la API de Azure denominada 'Graph' para dar de alta a los usuarios, opción que no me convence porque implicaría que estamos dando a todos los usuarios en nuestro dominio con una cuenta del tipo 'usuario@organizacion.com' lo cual termina produciendo que si tenemos muchos usuarios la gestión de los mismos sea más difícil, sería difícil diferenciar un usuario externo de uno interno. Además tiene otro inconveniente, estamos obligando al usuario externo a recordar una nueva dirección de correo, cuando al ser un usuario externo usualmente ya tendrá una cuenta de correo, tipo gmail, yahoo... o incluso una cuenta de Facebook. Mediante Azure Active Directory B2C podemos crear aplicaciones en las que los usuarios se autenticarán con sus cuentas, dejando en mano de Azure y en caso de usar una cuenta tipo Facebook también dejaríamos en sus manos la autenticación. Un manual de uso para esta tecnología la veremos también en anexo 'Segundo escenario'.

2.5. Protección de usuarios

En una empresa con pocos usuarios como es una PyME, los empleados no suelen tener tan delimitadas sus funciones como en una gran empresa en la que los empleados conocen sus competencias nada más entrar en la en ella. Al tener más funciones, los empleados conocen más sobre la empresa y puede llegar a ser muy perjudicial para la misma que se vean comprometidos, por lo que en el caso de que dicha situación llegue a ocurrir debemos de detectarlo lo antes posible para actuar con celeridad tomando las medidas oportunas. Como hemos visto en el capítulo anterior, los usuarios van a estar ubicados en Azure, por lo que es lógico pensar que Azure implementará métodos para auditar a los usuarios si cometen actividad sospechosa.

Aunque tengamos la cuenta de Azure Active Directory gratuita vamos a obtener ciertos informes como los que se muestran en la imagen, en los que podemos observar la hora y la aplicación en la que se ha registrado o si ha ocurrido un cambio de contraseña. Sin embargo, analizar estos reportes puede ser algo tedioso cuando el número de usuarios es considerable (Figura: Reportes básicos).

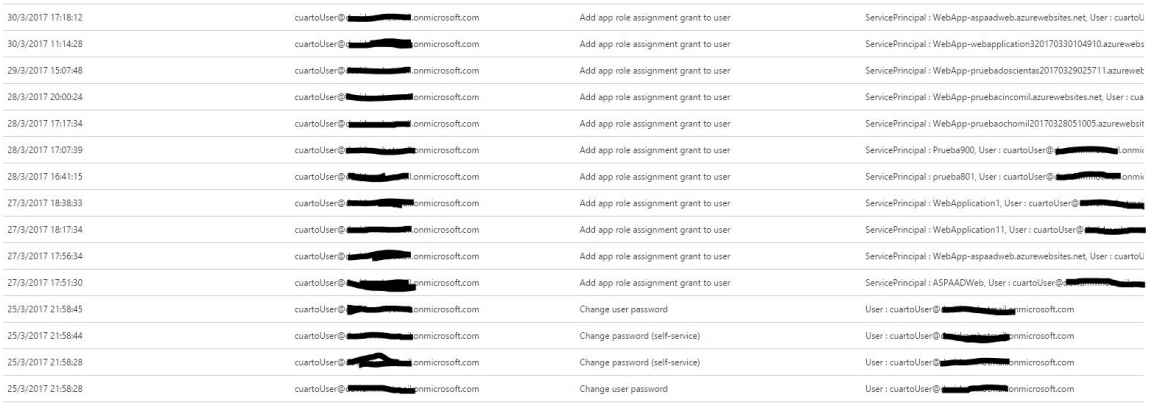


Figura 2.4: Reportes básicos

Sería interesante obtener más reportes, por ejemplo ¿Qué ocurre si un usuario se conecta desde su puesto de trabajo y cinco segundos más tarde desde Rumanía? Evidentemente su cuen-

ta se ha visto comprometida, o posee poderes sacados de un cómic. El mayor nivel de protección y reportes para usuarios se obtiene utilizando una característica de la suscripción premium P2, que nos permite elaborar acciones que se ejecutarán automáticamente cuando un usuario se vea comprometido. El precio de que este sistema haga una monitorización de un único usuario es de 7'59 euros al mes, lo cual es bastante caro si se aplica a toda la organización, pero es recomendable activar dicha característica para los usuarios que dispongan de información confidencial. Para activar la cuenta premium hemos de dirigirnos a la pestaña de AAD en el portal, y en la pantalla principal se nos mostrará un cuadro en el que se muestra aplicaciones empresariales, e iniciar una prueba gratuita. Siguiendo esos pasos nos activará una prueba gratuita de un mes para el usuario con el que estemos conectados de un mes de AAD P2. Una vez activada la característica hemos de instalar un servicio denominado Identity Protection [9] que es del que he hablado hasta ahora. Para instalar dicho servicio, pulsaremos sobre el icono '+' para añadir un servicio y escribiremos 'Azure Ad Identity Protection'. Seleccionaremos el servicio con el mismo nombre, y pulsaremos en 'Crear' en el panel que se despliega a la derecha. Sin realizar ninguna configuración adicional el servicio será desplegado, para acceder a dicho servicio, en el botón de 'más servicios' de la barra lateral izquierda escribiremos el nombre de éste servicio, y se abrirá la consola de administración. Desde dicha consola de administración, podemos observar en la pestaña de vulnerabilidades los usuarios que no tienen activado MFA (Visto en capítulos anteriores). Además, podemos observar una pestaña de 'políticas de riesgo en inicio de sesión' señalada con el icono de una llave. Desde esta pestaña, podremos configurar políticas que se aplicarán cuando un usuario se vea comprometido, por ejemplo, yo he creado una para que cuando un usuario tenga un riesgo medio o superior vea su cuenta bloqueada. Desde 'Usuarios' podemos configurar los usuarios que se verán afectados o excluidos por la política, en 'Condiciones' indicaremos el nivel de riesgo en cual se aplicará la política, desde 'Controles' la acción a emplear (Bloquear cuenta, exigir MFA...), y desde 'Revisar' se nos mostrarán los usuarios que se verían afectados por la política en el momento de la implementación. Los tipos de alertas se pueden dar debido a que un usuario se ha conectado desde una ip anónima, ha conectado desde un dispositivo infectado... `https://docs.microsoft.com/es-us/azure/active-directory/active-directory-reporting-risk-events` (Figura: Política de bloqueo).

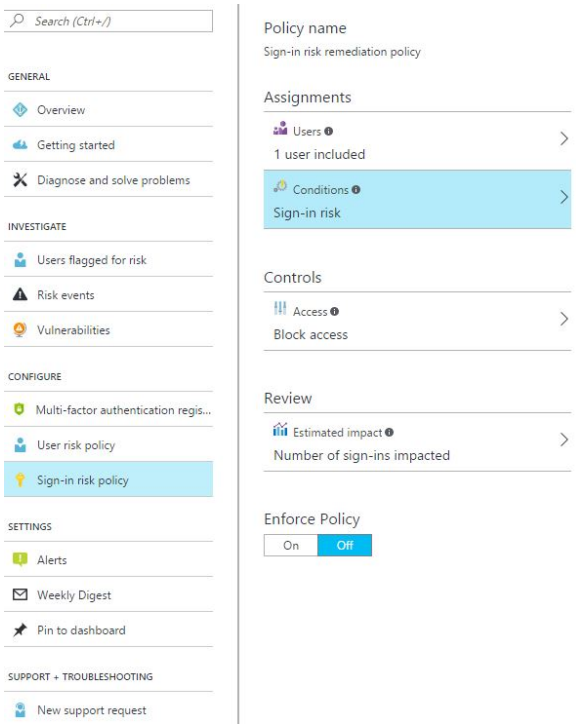


Figura 2.5: Política de bloqueo

Para probar este servicio me he conectado desde una máquina virtual en Holanda a una de mis aplicaciones, lo cual ha hecho saltar una alarma, para ver los usuarios marcados en riesgo por alguna alarma, iremos al panel de Azure AD Identity Protection, como se ve en la imagen 'Usuarios en riesgo' que nos sale en la primera pantalla, tenemos el usuario del cual Azure ha detectado algo extraño, si pinchamos en dicho cuadro veremos como se ha marcado a mi usuario por conectarse desde una ubicación poco habitual (Figuras: Usuarios en riesgo, Usuarios en riesgo 2).

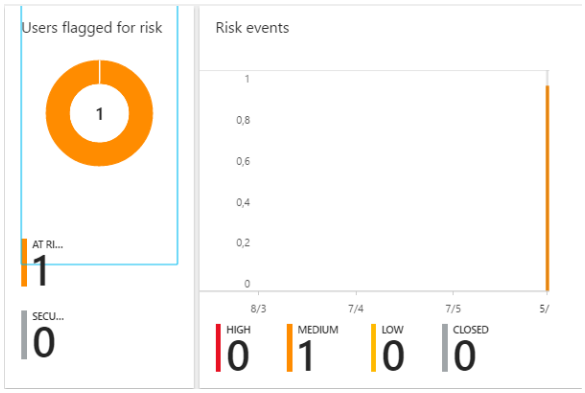


Figura 2.6: Usuarios en riesgo

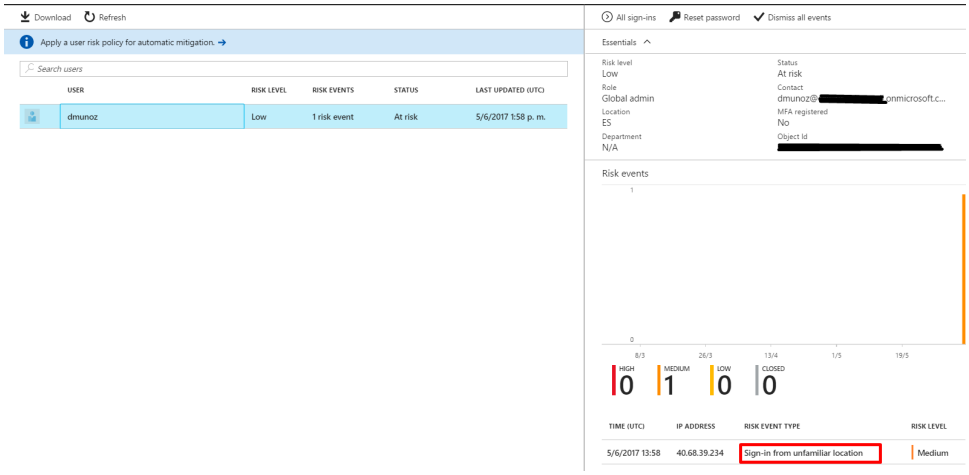


Figura 2.7: Usuarios en riesgo 2

2.5.1. Acceso condicional

Imaginemos ahora que tenemos desarrollada nuestra aplicación, la cual accede a datos confidenciales de nuestra compañía, por mucho que Microsoft nos asegure que la autenticación mediante su sistema es segura, hay muchos factores por los que un usuario puede ver comprometidas sus credenciales de acceso; si han visto la película 'Ahora me ves' los magos consiguen las credenciales del banco de un multimillonario sonsacándole inocentemente el nombre de su gato y de su tía, a esto se le conoce como ingeniería social habitual, al multimillonario lo desplu-man y, por mucho que su banco se esfuerce poniendo encriptación, firewalls y un nuevo sistema imaginario de computación cuántica, si alguien tiene las credenciales de acceso, accede.

Debemos tener en cuenta que este escenario es posible y que nuestros empleados pueden ser descuidados y comprometer sus credenciales, ahora hemos de pensar qué podemos hacer al respecto, una solución que nos da Azure es el acceso condicional, mediante el cual podemos crear una serie de reglas de acceso para nuestros usuarios. Por ejemplo, sabemos que un empleado tiene un teléfono con SO Android y que siempre se conecta a dicha aplicación desde nuestra oficina o desde su casa (Puede hacer teletrabajo). Si sabemos estas condiciones, si en un momento dado alguien accede con sus credenciales utilizando un dispositivo IOS desde China está claro que es un acceso que no se debería llegar a autorizar.

Esto lo podemos dirigiéndonos en el portal de Azure a 'Azure Active Directory', 'Enterprise applications', 'conditional access', 'policies'. En esta pantalla vamos a añadir una nueva política pulsando en 'New policy'. Aquí vemos las opciones que podemos configurar.

- Usuarios y grupos: Podemos aplicar la política a todos los usuarios, a grupos o usuarios específicos desde la pestaña 'include'. Desde la pestaña 'exclude' si hemos seleccionado un grupo y queremos que no se aplique a un usuario determinado podemos excluir a dichos usuarios. En mi caso seleccionaré a 'segunuser' . . .
- Cloud apps: Aquí seleccionaremos las aplicaciones a las que afectan esta política, en mi caso el Wordpress que alojé previamente. . .
- Conditions:
  - Sign-in Risk: Azure mediante algoritmos propios va incluyendo en un grupo de riesgo u otro a los usuarios de nuestra organización; por ejemplo, un usuario que siempre se conecta desde el mismo no presenta riesgo aparente, desde aquí podemos seleccionar

el nivel de riesgo con el que se empieza a aplicar la política, en mi caso elijo todos los grupos de riesgo debido a que quiero que se aplique en todo caso mi política.

- Device platforms: Plataforma desde la que se conecta el usuario. Por ejemplo, si sé que no tiene un equipo Windows puedo aplicar la política para cuando el usuario se conecte desde dicha plataforma.
- Locations: Ips desde las que se aplica la política, puedo excluir por ejemplo la IP nuestra organización ya que confío en que no haya conexiones maliciosas desde este entorno. En mi caso aplicaré la política a todas las ip.
- Client apps: Define si la política se aplica cuando nos conectamos desde una aplicación o desde un navegador

- Grant: Podemos bloquear acceso totalmente o pedir autenticación mediante MFA, algo que ya vimos. En mi caso bloquearé el acceso, pero es una medida muy útil pedir MFA, queda a elección del lector. ...

Si después de configurar una regla para 'segunUser' que impida el acceso desde ciertas direcciones IP para dispositivos Windows e intentamos acceder a dicha aplicación, se obtiene el siguiente error (Figura: Bloqueo de acceso).

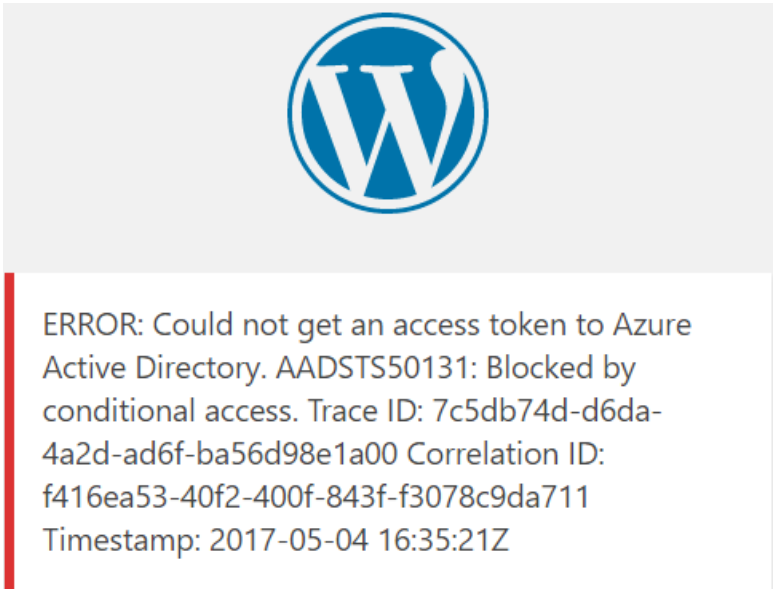


Figura 2.8: Bloqueo de acceso

Nota: Acceso condicional está en fase beta y se espera que se añadan bastantes características al margen de las comentadas, por lo que puede variar cuando el usuario intente configurar sus propias políticas.

2.6. Protección de la infraestructura

Como hemos comentado previamente, en cualquier punto de la infraestructura puede haber puntos que si no están bien protegidos pueden ser utilizados por un atacante para infiltrarse en nuestro sistema y causar graves daños. Hasta ahora hemos protegido a los usuarios, ciertas aplicaciones y el entorno de administración del sistema. Además, hemos dejado en manos de Microsoft parte de la responsabilidad de la seguridad de la empresa, pero como dijimos en el apartado de responsabilidades, si tenemos una máquina con un sistema operativo, nosotros

debemos de ser los encargados de la seguridad de ese sistema, o si administramos una base de datos, hemos de ser nosotros los que se encarguen de dicha seguridad. Esto puede suponer un alto coste en tiempo y económico, sobre todo para las compañías que tratamos en este escrito. Por ello Azure pone en marcha otro sistema que puede ayudarnos a proteger nuestro sistema, para ello monitoriza los servicios que alojamos en su plataforma continuamente y nos da consejos de seguridad sobre ellos.

Haciendo un inciso sobre esta última frase, seguramente eso de que una gran compañía monitorice los equipos puede no hacer mucha gracia al lector. Hay multitud de páginas en Internet que afirman que compañías como Google, Microsoft, Amazon... venden nuestros datos a los gobiernos y que por eso quieren monitorizarnos, pero nada más lejos de la realidad, esos datos se utilizan para mejorar los sistemas que utilizamos; gracias a lo que hoy en día se conoce como Big Data, que no es más que la recolección masiva de datos y su procesamiento mediante algoritmos de aprendizaje automático las compañías pueden saber dónde fallan sus productos sin necesidad de tener granjas de usuarios testeando los mismos. Una prueba de que por ejemplo Microsoft, la compañía que posee Azure intenta proteger los datos de los usuarios lo máximo posible es que se ha convertido en el primer gestor de *cloud computing* en cumplir con la nueva norma europea de le Regulación Europea de Protección de datos [10], algo así como la LOPD a nivel europeo, y seguramente los otros proveedores de *cloud* se encuentren trabajando en el mismo objetivo. El lector puede encontrarse también al tanto de las informaciones que salen de 'Wikileaks' referentes a que el gobierno americano mediante su agencia en la CIA tiene infectados la mayoría de dispositivos del mundo, no sólo ordenadores sino también móviles, e incluso televisores [11]. Este es un gran problema al que se enfrentan las compañías, podemos recordar noticias del gobierno americano intentando obligar a Apple a desbloquear un teléfono [12], si éstas compañías cedieran ante dichos gobiernos perderían credibilidad de cara a los clientes, por eso las desafían e intentan llevar a cabo maneras de protegerse, como mover el centro de datos a Alemania [13].

Volviendo al quid de la cuestión, la herramienta que tratamos en esta sección se denomina Azure Advisor la cual es una de las herramientas integradas en Azure que nos dará consejos sobre cómo mejorar aspectos sobre: Alta disponibilidad, Rendimiento, Costo de los recursos nuestra suscripción e incluso la seguridad.

Para acceder al panel de Azure Advisor, en el portal de Azure, en el panel de la derecha pinchamos en el icono con un búho y se nos abrirá el panel de recomendaciones (Figura: Inicio Advisor).

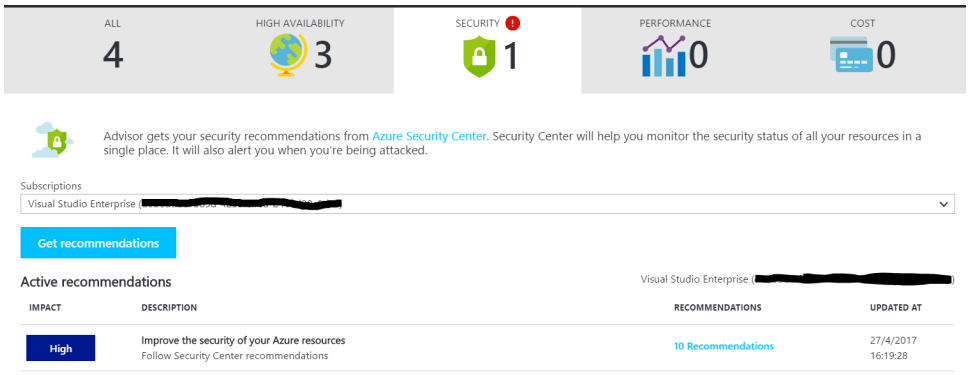


Figura 2.9: Inicio Advisor

Desde esta pantalla podemos habilitar Azure Security Center, una herramienta que nos da acceso a más herramientas, como son Key Vault, protección para máquinas virtuales, la autenticación en dos pasos o la que más nos importa.

Al habilitarlo, nos dará varias recomendaciones sobre todas las máquinas como podemos ver en la imagen (Figura: Recomendaciones Advisor).

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Add a Next Generation Firewall	SADEscenari...	Open	High	...
Enable Network Security Groups on subn..	default	Open	High	...
Enable Auditing & Threat detection on S...	servernames...	Open	High	...
Enable Auditing & Threat detection on S...	datanamesql2	Open	High	...
Apply disk encryption	C1Escenario1	Open	High	...
Enable encryption for Azure Storage Acc...	6 storage acc...	Open	High	...
Restrict access through Internet facing e...	SADEscenario1	Open	Medium	...
Enable Transparent Data Encryption	datanamesql2	Open	Medium	...
Provide security contact details	1 subscriptions	Open	Medium	...
Remediate OS vulnerabilities (by Microso..	UbuntuEscen...	Open	Low	...

Figura 2.10: Recomendaciones Advisor

Dos que me gustaría analizar en este capítulo serían la primera y la última. Si recordamos el capítulo del primer escenario, la máquina 'SADEscenario1' es la máquina que contenía el servidor Active Directory, por tanto, una máquina que es muy altamente recomendable de proteger mediante el uso de un firewall, Azure ha analizado el contenido de las máquinas y ha detectado un servidor Active Directory por lo que siguiendo las recomendaciones (Pinchando en la recomendación) llegamos a una pestaña de creación de un firewall (Figura: Recomendaciones de Firewall).

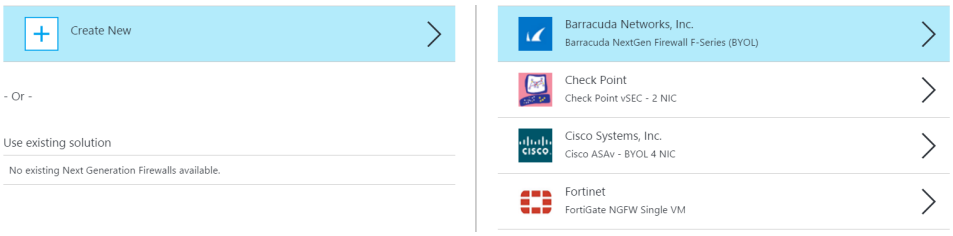


Figura 2.11: Recomendaciones de Firewall

Los Firewall que Azure nos ofrece son Firewall de siguiente generación de los que se habló en el capítulo anterior, de entre los NGFW que Azure nos ofrece `https://azuremarketplace.microsoft.com` el de Check Point, es el que tiene menor coste y nos ofrece protección contra ataques DDOS. Teniendo en cuenta que dicho servicio tiene un coste de aproximadamente 720 Euros al mes y mi cuenta de Azure dispone de 130 al mes no puedo finalizar la instalación, aunque hay diversas guías en internet para su instalación y configuración, citaré como más sencilla `https://docs.microsoft.com/es-es/azure/security-center/security-center-add-next-generation-firewall`

La segunda de las recomendaciones que he decidido analizar es la de 'Remediar vulnerabilidades del sistema operativo' y me gustaría analizarla debido a que la máquina alojada no contiene un sistema operativo Microsoft sino un ubuntu y podemos ver como Azure nos ofrece recomendaciones para todos los sistemas operativos que soporta Azure. Si desplegamos dicha opción veremos cómo se nos ofrece la manera de solucionar dicha vulnerabilidad y la razón para ello, si únicamente nos dijeran que tenemos una vulnerabilidad tendríamos que gastar tiempo en

ello, de esta manera obtenemos el problema y la solución. Si hacemos una búsqueda por internet de dichas vulnerabilidades, podemos observar que son recomendaciones reales de seguridad `https://wiki.ubuntu.com/Security/Features` (Figura: Recomendaciones Ubuntu).

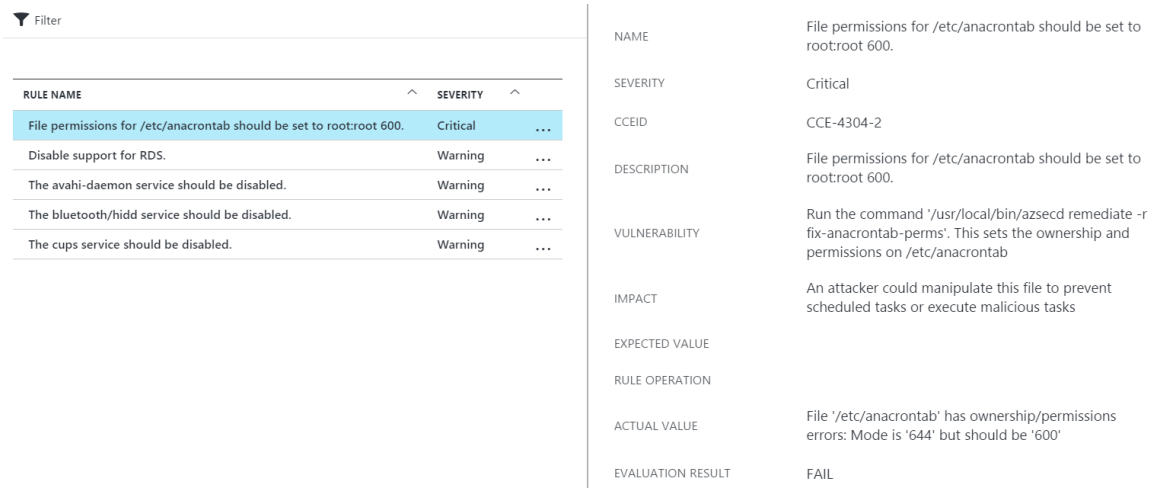


Figura 2.12: Recomendaciones Ubuntu

Como podemos observar, copiando el comando y ejecutándolo en una terminal se aplica sin ningún problema (Figura: Aplicando recomendación Ubuntu).

```
root@UbuntuEscenario1:/home/UbuEsce1# /usr/local/bin/azsecd remediate -r fix-ana
crontab-perms
2017/04/27 15:03:22 INFO: Performing baseline remediations. Detected Distro: Id=
ubuntu, Version=16.10
2017/04/27 15:03:22 INFO: Remediation 'fix-anacrontab-perms' has 1 actions to pe
rform: Fix anacrontab perms
2017/04/27 15:03:22 INFO: Running script:


if [ -e /etc/anacrontab ]; then
    chmod 600 /etc/anacrontab
fi
```

Figura 2.13: Aplicando recomendación Ubuntu

Nota: Si nada más aplicar las recomendaciones actualizamos el estado de las recomendaciones, observaremos que no han cambiado. Esto es debido a que Azure examina cada cierto tiempo nuestros recursos y debemos de esperar a que detecte que hemos realizado las medidas oportunas para mitigar los riesgos de seguridad de nuestro sistema.

Por último, aunque no tenga nada que ver con la seguridad directa de nuestro sistema, tenemos también la pestaña de 'Alta disponibilidad' en Azure Advisor la cual nos dará también recomendaciones como planear Backups de nuestras máquinas o realizar configurar para aumentar la tolerancia a fallos.

2.7. Protección de documentos

Hasta ahora hemos hablado de protección de infraestructuras, de usuarios y de aplicaciones, pero no hemos hablado de lo más importante (quitando a los empleados) que posee una compañía: su documentación. Da igual el tipo de empresa que usted posea, siempre tendrá información que no quiere que caiga en manos de su competidor. Una gran empresa con millones de empleados que fabrique un refresco de cola, no querrá que una sola de las fórmulas que utilizan para uno de sus múltiples productos, caiga en manos de otra empresa que venda productos de cola

ya que estamos hablando de una empresa con márgenes de beneficios mucho más amplios porcentualmente hablando que las compañías a las que representa el público dirigido en el presente trabajo. Imagine que cae en manos de la competencia el precio al que compra una materia prima antes de su compañía la transforme para revenderla. Si usted compra a ochenta y vende a cien y su competencia se entera, podrá comprar a ochenta y vender a noventa, quedándose así con todos los potenciales compradores de su compañía.

De tal manera la computación en la nube nos ofrece varias maneras de tener nuestros datos seguros.

2.7.1. Protección al enviar un documento

Seguramente conocerá la historia de la máquina Enigma. Durante la segunda guerra mundial, los Nazis desarrollaron un método para encriptar sus mensajes, cuando tenían el mensaje encriptado, lo transmitían mediante ondas de radio, de tal manera que todo el mundo podía recibir la comunicación pero sólo alguien con una máquina enigma tenía la capacidad de entender el mensaje. Ya sabemos que nuestros documentos son lo más valioso del mundo. Pero en algún momento podemos tener que dárselos a otra persona enviarlo por correo, y obviamente queremos asegurarnos de que dicho documento, aunque caiga en malas manos no se pueda ver su interior, Azure junto con la plataforma ofimática de Office 365 han creado una tecnología denominada Azure Information Protection que permitirá que sólo el usuario que nosotros deseamos pueda abrir un documento, e incluso que el documento se autodestruya en la fecha indicada. Dicha plataforma hace uso de un servicio denominado Azure RMS que servirá tanto para encriptar los documentos como para autenticar a la persona que los abre.

El problema de todo, es que solamente se puede utilizar este servicio con los documentos creados con la aplicación de Microsoft Office y hay que tener un usuario en Office365. Por lo que el sistema ofrece un rango limitado de uso, no podrá usarlo alguien que tenga por ejemplo una cuenta en Gmail. Como la instalación y configuración del servicio no es demasiado larga en lugar de crear un anexo especial veremos el uso en este mismo capítulo [14][15].

Nota: Este servicio incluye mucha más potencia de la que veremos, debido a que para ello hay que utilizar licencias que no tengo a mi disposición. La potencia añadida contendría opciones como proteger automáticamente los documentos que contengan DNI o cuentas bancarias y realizar seguimiento de quien intenta abrir dichos documentos, pero para utilizar este servicio hay que tener un tipo de cuenta de office 365 que se denomina Enterprise Mobility + Security E5.

Instalación

Además de tener Office instalado, necesitamos instalar un cliente que podemos descargar desde `https://www.microsoft.com/en-us/download/details.aspx?id=53018`.

Utilización del servicio

Si hemos seguido todos los pasos, podemos iniciar sesión en Microsoft Word (o cualquier otra aplicación) con uno de nuestros usuarios y abriremos el archivo que deseamos proteger. Si hemos instalado el cliente veremos en la barra superior un icono con forma de candado en el que pone 'Proteger' y se nos desplegará la siguiente ventana en la que seleccionaremos la protección del documento (Figura: Permisos sobre el documento).

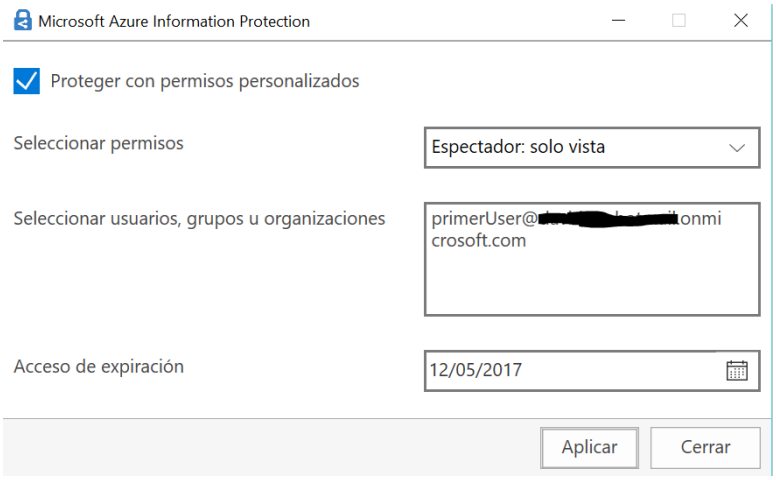


Figura 2.14: Permisos sobre el documento

En el desplegable tenemos las siguientes opciones:

- Solo vista: Los usuarios a los que demos permisos no podrán ni editar, ni copiar el contenido ni imprimir el documento (Aunque nada impide que le hagan una foto).
- Vista edición: Los usuarios con permisos podrán editar el contenido..
- Copropietario: Con todos los permisos.
- Solo para mí: Nadie salvo el usuario que crea el documento podrá abrirlo.

En el cuadro de texto introduciremos los usuarios, grupos u organizaciones a los que asignamos los permisos (En el caso de una organización podríamos su nombre de dominio) y en 'expiación', la fecha en la que queramos (en caso de quererlo) que se auto-destruya el documento. Hay que tener en cuenta que se destruyen todas las copias a partir de la cual se ha protegido el documento, es decir, si queremos que el documento se destruya y queremos mantenerlo, haremos una copia del documento original y sobre esa copia aplicaremos la protección.

Cuando guardemos el documento ya estará listo para ser enviado. Si un usuario con permisos para abrirlo lo abre no notará la diferencia con un archivo normal y corriente, en cambio si no tiene permisos, notará el siguiente comentario y no podrá ver el contenido (Figura: Documento restringido).

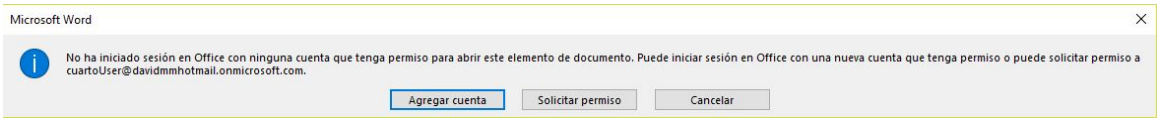


Figura 2.15: Documento restringido

Cifrado

Para explicar de manera sencilla el funcionamiento de este método de protección, vayamos por partes. En primer lugar tenemos un servidor RMS que instalaremos en nuestra cuenta de Azure que se encarga de dos tareas, la primera autenticar a los usuarios (para lo que hace uso de Azure AD, por lo que estos usuarios han de existir en nuestro Azure AD) y además envía a los usuarios (tanto el que encripta el documento como el que quiere abrirlo) unos certificados

que contienen claves para encriptar y desencriptar el documento. En segundo lugar tenemos al cliente el cual encripta el contenido del documento con una algoritmo de tipo AES de 256 bits. La clave de encriptación con una clave RSA de 2048 bits y la manda en un certificado SHA-256. Todo esto implica tener varios métodos de encriptación bastante poderosos pasando por un servidor el cual es Azure el que nos garantiza su seguridad.

2.7.2. Almacenamiento de los datos

Como ya hemos mencionado, el dato es uno de los bienes más preciados de las compañías y ya hemos visto como podemos trasladarlos de un lugar a otro aumentando la seguridad de los mismos. Pero hay otro problema ¿Dónde almacenamos los datos? Hoy en día existen muchos medios disponibles para esto, desde un disco duro hasta una cuenta en servicios como Dropbox. Pero los discos físicos tienen el inconveniente de que ocupan espacio y que somos nosotros los que tenemos que hacernos cargos de la seguridad de los mismos. Servicios como Dropbox tienen otro problema, no es un problema de seguridad ya que estos servicios proveen de capas de seguridad a la hora de securizar las instalaciones. Es un problema de permisos, durante todo este documento hemos estado utilizando un mismo servicio, y ahora queremos seguir haciendo lo mismo para hacer más fácil la administración.

Azure tiene un servicio de almacenamiento que hemos venido usando hasta ahora sin darnos cuenta. Este servicio se conoce como 'Azure Storage Account' y en diversos servicios como éste, están almacenadas las máquinas virtuales que hemos creado, así como las web que hemos creado, son por así decirlo contenedores, y podemos almacenar cualquier cosa. Pues también podemos utilizarlo para almacenar ficheros y crear permisos para que los usuarios accedan a los ficheros que almacenamos. Dicho servicio en mi opinión no está muy pulido para compartir de manera sencilla fichero para que los usuarios puedan trabajar con ellos, el acceso a fichero tiene más desarrollo de cara a acceder a los mismos mediante programas propios de la empresa, ya que la API tiene muchas opciones. Para acceder a estos archivos, necesitamos de un programa instalado en el cliente, en el cual para acceder a los recursos de manera sencilla se realiza mediante una 'URL'. Ésta contiene permisos a los recursos en lugar de utilizar un usuario de los que hemos creado en nuestro AAD. Otro inconveniente es que no podemos asignar permisos a las carpetas que almacenamos en los contenedores, sino que asignamos los permisos al contenedor entero, por lo que tendremos que crear varios contenedores según nuestros objetivos.

Al igual que el anterior utilizar este recurso es sencillo, por lo que no veremos el manual en un anexo sino a continuación.

En primer lugar vamos a crear un contenedor, para ello en la pestaña de 'más servicios' del panel lateral izquierdo del portal de Azure y buscaremos 'Storage Account'. Si hemos instalado máquinas virtuales veremos varios de los contenedores ya creados en la ventana que se abre. En estos contenedores podemos guardar ficheros, pero por un tema de orden es mejor crear contenedores con la finalidad de guardar ficheros. Pulsaremos en el botón 'Añadir' [16].

- Nombre: Este será el nombre del recurso
- Modelo de despliegue: Clásico o manejador de recursos, marcaremos el último dado que nos permite encriptar el contenido del contenedor.
- Tipo de cuenta: Propósito general o por blobs, marcaremos el primero ya que nos permite almacenar ficheros.
- Rendimiento: Estándar o premium. Marcaremos el primero, ya que el segundo se almacena en SSD y es exclusivo para almacenar máquinas virtuales.

- Replicación:

  - Almacenamiento localmente redundante (LRS): Realiza múltiples copias asíncronas de los datos dentro de un solo centro de datos.

  - Almacenamiento con redundancia de zona (ZRS): Almacena tres copias de datos en varios centros de datos de la misma región o regiones diferentes. Solamente para blobs en bloques.

  - Almacenamiento geográficamente redundante (GRS): Igual que LRS, más copias asíncronas múltiples en un segundo centro de datos situado a cientos de millas.

  - Almacenamiento con redundancia geográfica con acceso de lectura (RA-GRS): Igual que GRS, más acceso de lectura al centro de actor secundario ...

  En mi caso marcaré LRS. Es el más barato y no necesito que los datos se encuentren en todo momento disponibles.

- Encriptación: Habilita o deshabilita la encriptación de los ficheros, marcaremos habilitar para que nuestros ficheros se encuentren más seguros.

- Suscripción: Suscripción en la que se realiza el pago.

- Localización: Centro de datos en el que se almacena el contenedor.

Ahora nos descargaremos e instalaremos el cliente de 'Azure Storage Explorer' desde `http://storageexplorer.com/` para poder acceder a los recursos. Si iniciamos sesión como el administrador podremos ver tiene acceso a todos los contenedores creados, mientras que si iniciamos con otro usuario no vemos ningún contenedor en el desplegable (Figura: Contenedores administrador).

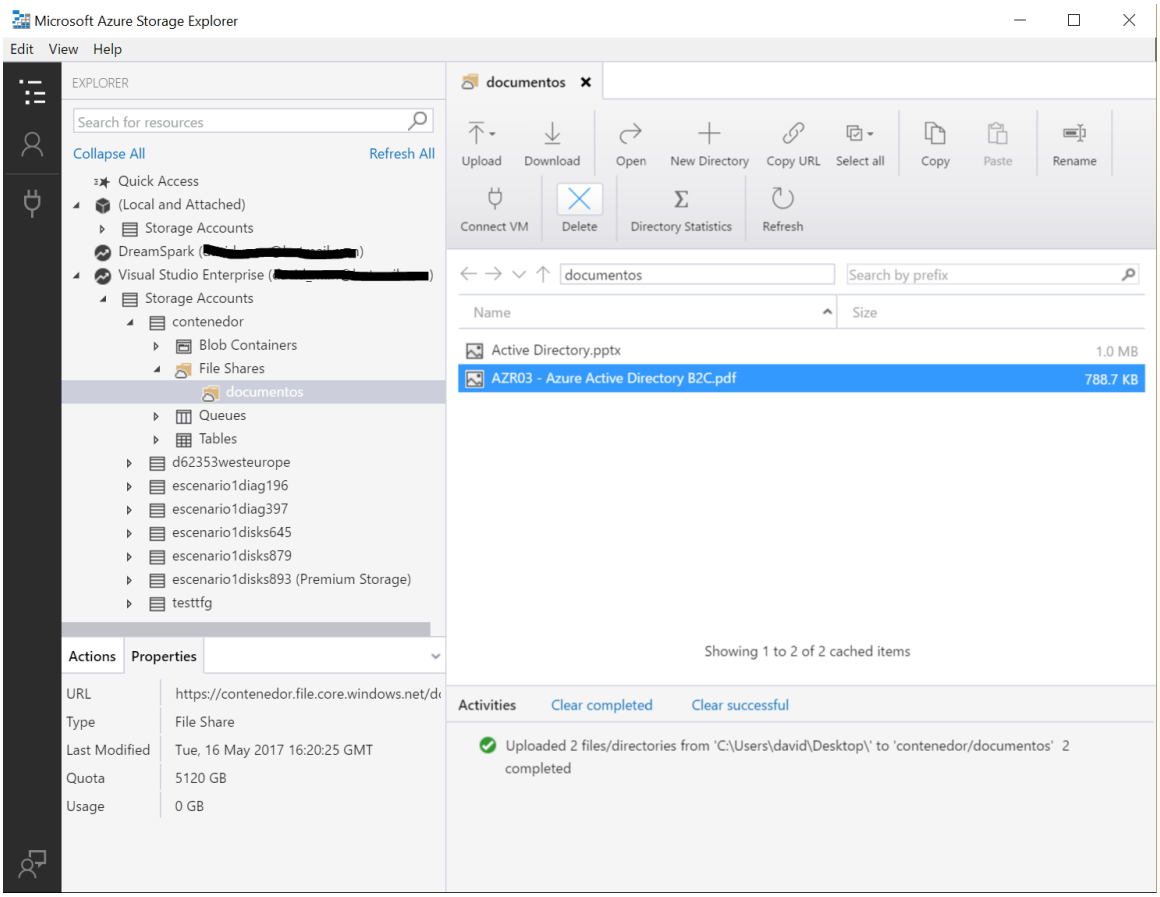


Figura 2.16: Contenedores administrador

Ahora para conceder permisos, debemos de volver al portal de Azure y seleccionar nuestro contenedor. Y seleccionaremos la opción 'Firma de acceso compartido' para crear un enlace al recurso y sus permisos. Podremos seleccionar los permisos de acceso, mínimo debemos de seleccionar listar y leer. Como vamos a almacenar ficheros sólo permitiremos este servicio. También podemos seleccionar la fecha desde la que se puede acceder a esos ficheros y hasta cuando se puede acceder, lo cual es útil si vamos a compartir temporalmente los recursos con alguien externo a la compañía, además podremos seleccionar la IP pública de nuestro router si queremos que sólo se acceda desde la compañía, por si dicho enlace cae en malas manos. Además seleccionaremos que sólo se puede utilizar Https para que todas las conexiones al usar dicho servicio sean cifradas. A la hora de subir archivos será más lento, pero también mucho más seguro, ya que si un ciberdelincuente intercepta la comunicación no podrá ver su contenido (Figura: Permisos SAS).

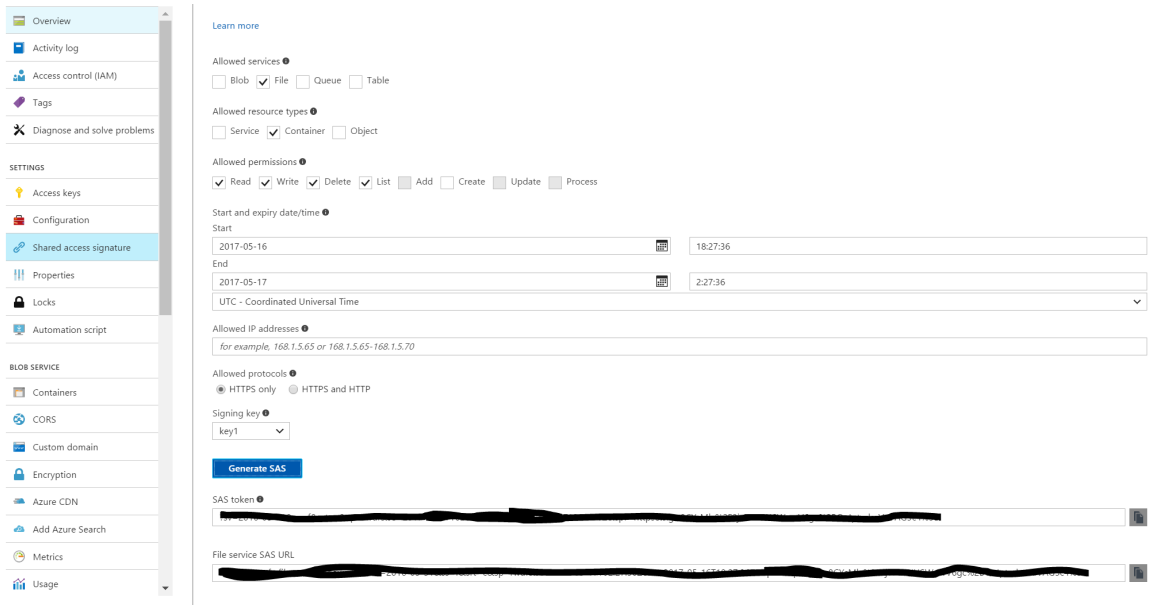


Figura 2.17: Permisos SAS

Una vez hayamos generado los permisos, pincharemos en 'generar key' y copiaremos la segunda que aparece: 'File service SAS URL'. Para poder utilizar dicha clave y poder acceder a los recursos iremos a la aplicación de Azure Storage Explorer, a la izquierda pulsaremos en el botón del enchufe 'Connect to Azure Storage'. Marcaremos 'Use a shared access signature', en la siguiente pantalla: 'Use a SAS URI' y pegaremos la URI que hemos copiado previamente. Cada contenedor almacena hasta cinco terabytes de información, pero las operaciones tienen un coste, el cual analizaremos en el próximo capítulo.

2.7.3. Cifrado

Los datos en el servidor están cifrados con AES de 256 bits [17], un cifrado de alta seguridad. La protección de los datos en el tránsito se compone de varios pasos [18].

Primero se cifran los datos antes enviarse:

1. 'La biblioteca de cliente de almacenamiento de Azure genera una clave de cifrado de contenido (CEK), que es una clave simétrica de un solo uso. Dicha clave está compuesta de un vector de inicialización (IV) aleatorio de 16 bytes, junto con una clave de cifrado de contenido (CEK) aleatoria de 32 bytes.'

2. 'Los datos de usuario se cifran mediante esta CEK.'

3. 'Se encapsula la CEK (cifrada) con la clave de cifrado de clave (KEK). La KEK se identifica mediante un identificador de clave y puede ser un par de clave asimétrico o una clave simétrica que puede administrarse de forma local o guardarse en Almacén de claves de Azure. La propia biblioteca de cliente de almacenamiento no tiene nunca acceso a la KEK. La biblioteca invoca el algoritmo de encapsulado de clave proporcionado por Almacén de claves. Los usuarios pueden elegir utilizar proveedores personalizados para el ajuste y desajuste clave si lo desean.'

4. 'A continuación, se cargan los datos cifrados en el servicio Almacenamiento de Azure. La clave encapsulada y algunos metadatos adicionales de cifrado se almacenan como metada-

tos (en un blob) o se interpolan con los datos cifrados (cola de mensajes y las entidades de tabla).'

A continuación se descifran al llegar:

- 'La biblioteca de cliente asume que el usuario está administrando la clave de cifrado de claves (KEK), ya sea localmente o en almacenes de claves de Azure. El usuario no necesita conocer la clave específica que se usó para el cifrado.'
- 'La biblioteca de cliente descarga los datos cifrados junto con cualquier material de cifrado que esté almacenado en el servicio.'
- 'A continuación, la clave de cifrado de contenido encapsulado (CEK) se desencapsula (descifra) usando la clave de cifrado de claves (KEK). Aquí nuevamente, la biblioteca de cliente no tiene acceso a la KEK. Simplemente, invoca el algoritmo de desencapsulado personalizado o el del proveedor de Key Vault.'
- 'La clave de cifrado de contenido (CEK) se usa entonces para descifrar los datos cifrados del usuario.'

3

¿Cuál es el coste de la nube?

En los capítulos previos, se han visto multitud de tecnologías que ayudan a hacer más seguros varios de los componentes de nuestra infraestructura. En este capítulo, examinaremos los costes de utilizar dichas tecnologías y lo compararemos con el coste de tener soluciones parecidas en un entorno On premise. En primer lugar hay que decir que en los servicios en la nube se paga habitualmente por el uso por minuto que se hace de una tecnología, es decir, si tenemos una máquina virtual pero solamente la encendemos un día en todo el mes, pagaremos un día de uso no un mes.

Azure provee de una herramienta calculadora que utilizaré para este capítulo. La podemos encontrar en `https://azure.microsoft.com/es-es/pricing/calculator/` y en ella agregaremos los elementos que queramos de todos los productos que ofrecen y nos mostrará el precio por horas o días. Como mucho se nos muestra un mes, dado que los precios los actualizan con dicha frecuencia.

3.1. Cuenta en la nube

Está claro que lo que primero que necesitamos es una cuenta en un proveedor de computación en la nube, en mi caso he utilizado Azure. Dicha cuenta es gratuita, tanto en el proveedor que yo he utilizado como en el resto.

3.2. Virtualización

Hemos visto que podemos mejorar la seguridad de nuestra infraestructura instalando servicios en máquinas virtuales en la nube. En esta sección vamos a comparar los costes de tener una máquina virtual alojada en Azure con lo que nos costaría un servidor con las mismas características.

Lo primero que tenemos que decidir es el propósito del equipo servidor que necesitamos. Dado que muchas empresas optan por tener un servidor que albergue máquinas virtuales para virtualizar sus servicios optaré por dicho escenario. Dado que va a ser un servidor que simplemente servirá para albergar máquinas virtuales, podemos optar por tener un sistema operativo

Ubuntu, el cual tiene licencia gratuita y no consume tantos recursos como un sistema operativo Windows Server. Ahora pasemos a analizar el coste de tener nosotros dicho servidor o alojarlo en la nube

3.2.1. Coste de la virtualización

En primer lugar Azure tiene varios niveles de máquinas virtuales [19].

- Uso general: Uso equilibrado de la CPU en proporción de memoria. Ideal para desarrollo y pruebas, bases de datos pequeñas o medianas, y servidores web de tráfico bajo o medio.
- Proceso optimizado: Uso elevado de la CPU en proporción de memoria. Bueno para servidores web de tráfico medio, aplicaciones de red, procesos por lotes y servidores de aplicaciones.
- Memoria optimizada: Memoria alta en proporción de núcleo. Excelente para servidores de bases de datos relacionales, memorias caché de capacidad media o grande y análisis en memoria.
- Almacenamiento optimizado: Alto rendimiento de disco y E/S. Perfecto para bases de datos SQL y NoSQL y macrodatos.
- GPU: Máquinas virtuales especializadas específicas para la representación de gráficos pesados y la edición de vídeo. Están disponibles con uno o varios GPU.
- Proceso de alto rendimiento: Máquinas virtuales de CPU más rápidas y eficaces con interfaces de red de alto rendimiento opcionales (RDMA).

Una PyME, por lo general va a utilizar máquinas de uso general, que coincide además con nuestro escenario de virtualización, por lo que vamos en centrarnos en ella.

El nombre de las máquinas de uso general comienza por A o D. Las máquinas tipo A son básicas mientras que las de tipo D más avanzadas, acaban de salir las de nueva generación Dv2, que tienen carasterísticas superiores a las de la primera generación y son más baratas por unos céntimos a la hora (quizás consumen menos energía). Dado que nuestro servidor es para alojar máquinas virtuales, tenemos que darle bastante memoria RAM, y no necesitaremos demasiados núcleos. Por todo esto elegimos una máquina con 28GB de RAM y 8 núcleos. Si buscamos algo semejante obtenemos la d3 v2 con un coste de 146,82 euros, que nos incluye un disco duro SSD de 400 GB y una cuenta de almacenamiento, además la memoria RAM es DDR4 y la CPU de dicho servidor un E5-2673 v3 de intel a 2'4GHZ. [20].

Las cuentas de almacenamiento tienen un coste [21]. Hasta 1TB de 0'0822 euros el GB para discos con redundancia geográfica. Si tenemos 1TB de información (esto es mucha información para una PyME, pero redondearemos por lo alto) para almacenar un disco con 1Tb necesitamos 82 euros al mes. Hay que tener en cuenta que por cada transferencia de datos se cobra 0,000304 euros por cada 10000 operaciones de lectura/escritura.

Por todo esto, pongamos que este servidor nos cuesta 228 euros al mes tener dicho servidor en la nube, lo cual representa 2736 euros al año.

3.2.2. Coste On premise

Buscaremos un servidor HP con características lo más similares posibles en la web de HP `store.hp.com`, podemos tomar el HP ProLiant DL380. Un servidor con características similares

aunque con un procesador un bastante peor (515 euros de diferencia en `/starmicroinc.net/` tendríamos un servidor de 1966,11 euros a los que añadimos 515 euros de diferencia de CPU, 246 euros de un HDD de 1TB de capacidad (en `store.hp.com`) y 446 euros en un SSD. Además, hemos de tener en cuenta que dicho servidor consume energía, al tener una fuente de alimentación de 500W. Si miramos el precio de la luz en `http://comparadorluz.com` estamos gastando 25 euros al mes en dicho servidor lo cual hace un total de 300 euros al año aproximadamente en electricidad y 3173 en el servidor.

3.2.3. Amortización

Tardaríamos 15 meses en consumir el coste de un servidor de estas características y cuando compramos un servidor esperamos que nos dure por lo menos dos años, por lo que el servidor en la nube nos costaría 1.824 euros más que tener el servidor en esos dos años.

3.2.4. Azure Active Directory y autenticación en dos pasos

Hemos visto también que Azure Active Directory es un servicio de auteticación. Dicho servicio tiene diversos planes incrementales con coste por cada usuario:

- Gratuito: Permite almacenar 500000 usuarios, autenticación con SSO o aplicaciones B2C, informes de seguridad básicos.
- Básico (0,884 euros usuario al mes): Esta opción permite personalizar la página de autenticación cuando utilizamos dicha característica.
- Premium P1 (5,06 euros usuario al mes): Permite técnicas más avanzadas de autenticación en dos pasos, acceso condicional y nos da informes de seguridad avanzados.
- Premium P2 (7,59 euros usuario al mes): Permite el uso de Identity Protection.

En mi opinión el servicio P1 es muy recomendable, ya que si creamos una buena política de reglas con acceso condicional nuestros usuarios se conectarán de manera segura. En caso de que sus credenciales se vean comprometidas los atacantes no podrán hacer uso de dichas credenciales.

El coste de utilizar la autenticación en dos pasos tal y como la hemos visto es de 1,181 euros al mes.

3.3. Protección de datos

En primer lugar, el servicio que hemos utilizado para proteger documentos a la hora de enviarlos es gratuito, sin embargo el usuario debe tener una cuenta de Office 365 para poder utilizar aplicaciones como Word o Excel, por que como mínimo deberemos tener una cuenta que cuesta entre 12 y 35 euros por usuario al mes.

También hemos utilizado cuentas de almacenamiento para securizar nuestros datos. Almacenar datos en la nube tiene un coste [21], como hemos utilizado este servicio para almacenar datos con un disco con redundancia geográfica analizaremos esos datos.

- 0,085 euros por GB, lo que implica 85 euros por un TB almacenado en la nube, un disco duro en la tienda de HP tiene un precio más elevado, el más barato nos costaría 140 euros. Hay bastante diferencia de precio, sin embargo el almacenamiento en la nube tiene más costes.

- 0,0253 euros por cada 10000 operaciones de crear una carpeta o subir un archivo.
- 0,0127 euros por cada 10000 operaciones de listado.
- 0,0013 euros por cada 10000 operaciones restantes, excepto eliminado de datos que es gratuito.

3.4. Aplicaciones Web

Las aplicaciones web que hemos desarrollado las hemos alojado en un recurso denominado 'App service', estos servicios tienen varios niveles:

- Gratuito: 1GB de almacenamiento, nada más que eso. No da soporte para tener la aplicación en nuestro propio dominio ni para SSL, no lo recomiendo más que para entorno de pruebas.
- Básico: 10GB de almacenamiento, admite dominios propios, SSL y soporta tres aplicaciones. Los precios van desde los 27 euros al mes con 1 núcleo y 2GB de RAM hasta los 110 euros con 4 núcleos y 7 GB de RAM.
- Estándar: 50GB de almacenamiento, dominios propios, SSL, backups diarios, balanceador de carga y autoescalado. Precios desde los 27 euros a 150 euros con las mismas condiciones de CPU y memoria que en el paso anterior.
- Premium: 250 de almacenamiento, dominios propios, SSL, autoescalado, espacio para 20 aplicaciones y 50 backups diarios. Desde los 188 euros a los 752 euros.

En mi opinión, el mejor plan es el estándar: El autoescalado permite que si tenemos un pico de peticiones se replique nuestro servidor para atender dichas peticiones, lo cual es muy útil para evitar que nuestro servidor se caiga en momentos puntuales. Si por ejemplo tenemos una web de alquiler de esquíes, sabemos que en periodo invernal tendremos muchas peticiones mientras que en periodo estival apenas tendremos peticiones. Podemos configurar Azure para que si se supera el 80 % de uso de CPU, se levante otra instancia para atender peticiones, se nos cobrará el uso de este nuevo servidor únicamente durante el pico de peticiones, no durante el resto del mes. Este es un escenario que únicamente se puede obtener teniendo nuestro servicio en la nube.

3.5. Uso del ancho de banda

Como mencionamos en el primer capítulo, todas las aplicaciones hacen uso de ancho de banda de los recursos de Azure, y se nos cobra por GigaByte utilizado siguiendo la siguiente escala:

- Primeros 5 GB/mes: Gratuito.
- 5 GB - 10 TB /mes: 0,074 euros por GB.
- Siguientes 40 TB (10 - 50 TB)/mes: 0,07 euros por GB.
- Siguientes 100 TB (50 - 150 TB)/mes: 0,06 euros por GB.
- Siguientes 350 TB (150 - 500 TB)/mes: 0,043 euros por GB.

Esto nos indica que si no tenemos demasiado tráfico, nuestra aplicación puede costarnos entre 0 y 74 euros al mes, a lo que habría que añadir el coste del alojamiento detallado en el punto anterior.

4

Problemas de la nube y cómo afrontarlos

4.1. Introducción

¿Es migrar a la nube la solución a nuestros problemas de seguridad? Como ya se ha comentado en capítulos anteriores la seguridad total no existe, la nube es un nuevo escenario y como todo nuevo escenario tiene sus desventajas sobre todo sino utilizamos la potencia al completo que nos ofrece la tecnología.

4.2. Separación de poderes

Uno de los principales problemas que trae consigo Azure es que para su administración se requiere utilizar la página web de Azure, `portal.azure.com` y desde ahí será desde donde administremos todos los recursos. Podemos crear, modificar e incluso eliminarlos, lo que supone varios problemas que iremos examinando.

El primer problema con el que nos encontramos tiene relación con el diseño. Cuando diseñamos un sistema para que sea lo más seguro posible lo hemos de diseñar teniendo en cuenta que no será cien por cien seguro y que en algún momento puede ocurrir una brecha en la seguridad del sistema. Si un administrador utiliza una única cuenta para todos los recursos de la empresa y un atacante consigue sus credenciales, al ser únicas todo el sistema está en peligro e incluso puede que no nos demos cuenta de que hemos tenido una brecha de seguridad, ya que los discos en los que residen nuestros recursos pueden ser clonados y descargados lo cual supondrá un aliciente para otras compañías.

Cuando montamos equipos físicos nos encontramos con una situación similar. Supongamos que en nuestra empresa únicamente disponemos de un servicio web y de una base de datos a la que accede la web, si ambos recursos residen en la misma máquina si la máquina sufre una brecha de seguridad ambos servicios quedan totalmente expuestos ¿Cuál es la solución para dicho escenario? Obviamente utilizar la estrategia 'Divide y vencerás', hacer que cada recurso resida en una máquina distinta y cada máquina y servicio tendrá un usuario y contraseña distinta.

Pues con Azure deberemos de utilizar la misma técnica, podemos instalar cada servicio en diferentes suscripciones y hacer que se comuniquen mediante redes internas o VPN. Podríamos

pensar que utilizar dicha técnica puede ser costoso, pero realizar dicha separación tiene el mismo coste que no realizarla ya que disponer de una cuenta de Azure no tiene gastos, el total se cargará por los recursos utilizados mientras que utilizar la misma estrategia con servidores físicos nos costará el precio de otro servidor y los costes energéticos que eso conlleva.

El hecho de poder acceder desde un portal de internet puede ser una gran ventaja: podemos conectarnos desde cualquier equipo con conexión a Internet. Pero hay que tener en cuenta una cosa, no sabemos si la máquina que estamos utilizando puede ser vulnerable o no. Cada vez que nos conectamos desde una máquina distinta aumenta la probabilidad de conexión desde un equipo infectado, la mejor opción es que el administrador realice conexiones al portal, siempre desde la misma máquina y que esta máquina tenga un este único propósito.

Por último, sería recomendable añadir una capa de seguridad más, cuando hablamos de autenticación, solemos pensar en una contraseña, pero también podemos utilizar algo que tenemos (un móvil, una tarjeta...) o algo que somos (una huella dactilar, retina...) Si juntamos dos de estas opciones para autenticarnos en sistemas clave, será mucho más difícil para un atacante entrar al sistema, puede que consiga la contraseña, pero si en el momento en que el usuario introduzca su usuario y contraseña tenemos que efectuar alguna acción desde un dispositivo móvil el usuario deberá de robar además dicho dispositivo. Podemos ver un manual sobre cómo utilizar esta tecnología para acceder al portal de administración de Azure en el capítulo de Autenticación multi factor en el portal de Azure.

4.3. Nuevos actores en escena

En el capítulo posterior se habla de cómo migrar parte o toda nuestra plataforma a Azure puede ayudarnos a conseguir más seguridad en nuestro entorno, pero esto conlleva la aparición de nuevos actores a escena y eso no es realmente deseable ya que, en nuestro de datos hay menos factores coexistiendo, tenemos nuestra red, nuestros servidores y los usuarios que acceden a ella, sabemos y podemos identificar fácilmente a estos actores, pero al portar servicios a Azure estaremos usando la red de Azure, los servidores de Azure y seremos un usuario más. En este capítulo veremos dos problemas fundamentales que entraña esta situación.

4.3.1. Aislamiento

El primero de nuestros problema es que estaremos utilizando otra infraestructura y no seremos los únicos. Imaginemos que vivimos en un pueblo, cada habitante del pueblo tiene su parcela en la que cultiva sus productos, los cuales vende a sus clientes. Esta analogía representa a la empresa que ofrece servicios a sus clientes teniendo los servidores físicamente en su oficina. Dicho habitante será el encargado no sólo de producir productos sino de proteger su parcela para que nadie le robe lo que en ella cultiva, puede poner perros, vallas eléctricas... Pero sigue siendo una persona (O unas pocas si contamos a su familia) la que se encarga de proteger el entorno teniendo en cuenta que hay muchas personas fuera de la finca que quieren robar en la finca (Ciberdelincuentes). Un día llega al pueblo una gran compañía la cual ofrece un espacio para que todos cultiven productos y además se hará cargo de la protección de los mismos. Es un invernadero gigante y los habitantes sólo van allí, reservan un espacio y cultivan sus productos, ahora hay cámaras de seguridad, guardias con metralletas las 24 horas, sensores infrarrojos y todo lo que os podáis imaginar, parece mucho más seguro, pero... Todos los productos están ahora en el mismo lugar, ahora los atacantes saben dónde están concentrados todos los productos y sólo es cuestión de medios que consigan acceder al recinto, sobre todo porque ahora van a conseguir un mayor beneficio. No tiene sentido excavar un túnel de 2 kilómetros para llegar a tu parcela ya que pueden saltar tu valla y robarte. Pero sí que tiene sentido hacerlo para conseguir todos

los productos de todos los habitantes del pueblo. Este concepto es el que usan las empresas y denominan ROI (Return on investment) o lo que es lo mismo: lo que voy a ganar por lo que voy a invertir. Seguro que el lector ya se ha percatado de la analogía, Microsoft obviamente es la gran compañía y Azure el nombre del invernadero. Está claro que debemos de contemplar este escenario como una cuestión de confianza. ¿Confiamos más en nosotros para defendernos de ataques más pequeños que en Azure para ataques a gran escala? Pues no debemos de migrar a Azure, pero si por el contrario consideramos que puede protegernos mejor de ataques externos debemos migrar. Todas las compañías van a intentar protegerse de los ataques que pueden causar el tener varios inquilinos en sus nubes y la manera que buscan para ello es la misma que en cualquier tipo de sistema, aislar unos recursos de otros, por ejemplo: Azure implementa el control de acceso de red y la segregación mediante aislamiento de VLAN, listas ACL, equilibradores de carga y filtros IP. Restringe el tráfico externo que entra en los puertos y protocolos en las máquinas virtuales que defina. Azure implementa filtrado de red para impedir tráfico falsificado y restringe el tráfico entrante y saliente a los componentes de plataforma segura. Se implementan directivas de flujo de tráfico en los dispositivos de protección de límites que deniegan el tráfico de forma predeterminada. La traducción de direcciones de red (NAT) se usa para separar el tráfico de red interno de tráfico externo. El tráfico interno no es enrutable externamente. Las direcciones IP virtuales que sean enrutables externamente se traducen en direcciones IP dinámicas internas que solo se pueden enrutar en Azure. El tráfico externo a máquinas virtuales de Azure atraviesa el firewall mediante listas ACL en enrutadores, equilibradores de carga y conmutadores de nivel 3. Solo se permiten determinados protocolos conocidos. Las ACL se usan para limitar el tráfico procedente de las máquinas virtuales invitadas a las otras VLAN usadas para la administración. Además, el tráfico filtrado a través de filtros IP en el sistema operativo host limita aún más el tráfico en vínculos de datos y niveles de red. [22].

4.3.2. Privilegios entre recursos

Para entender el segundo de los problemas que surge volvamos a nuestro ejemplo anterior, a nuestro invernadero. Supongamos que la empresa para cedernos una parcela simplemente nos pide una tarjeta de crédito (ya que exige pago) y nuestro nombre. Nadie ha dicho que no nos podemos inventar nuestro nombre, al igual que podemos crear cuantas veces queramos un usuario en cualquier plataforma. A la compañía no le interesa quien seamos, simplemente que paguemos rigurosamente, una vez hemos pagado nuestra parcela vamos a ella, y nos encontramos con que hay un muro de hormigón separando nuestra parcela de las demás de tal manera que no las vemos, pero sabemos que están ahí, así que podemos imaginar métodos muy imaginativos para robar las zanahorias al vecino tales como escalar el muro o cavar un tunel. En las plataformas en la nube sucede exactamente lo mismo, cuando nosotros alquilamos un servicio estamos alquilando un porcentaje en un servidor de máquinas virtuales y no sabemos qué máquinas virtuales contiene el servidor ni quien las usa. La virtualización es un manera muy popular para intentar aumentar la seguridad, no sólo porque se trata de un sistema aislado sino porque determinado malware puede actuar de manera inocente cuando se ejecuta en un entorno virtual para no ser detectado [23], pero esto no significa que sea un entorno seguro que nos proteja de toda adversidad ya que existen una serie de ataques para vulnerar la seguridad que la máquina que hospeda a la máquina virtual y conseguir privilegios para penetrar el resto de máquinas vecinos [24]. Obviamente contra dichos ataques los proveedores de servicios en la nube también se protegen. Azure crea cuatro anillos con distintos niveles de privilegios. En el anillo con menos privilegios, coloca las máquinas virtuales que van a albergar las aplicaciones de tipo SaaS, de tal manera que no se pueda acceder ni a la aplicación ni a la red que alberga; en el siguiente anillo coloca las máquinas que contienen PaaS; en el siguiente IaaS; para finalizar hay un último anillo el propio equipo físico que albera y gestiona el resto de anillos. Para aislar todos los anillos entre sí, el anillo con más privilegios contiene un firewall contra ataques de tipo hypervisor. Por último se usa una última medida

de protección llamada 'Controlador de tejido' que es la encargada de asociar permisos entre el servicio utilizado y los recursos del sistema, esto impide que sea directamente el recurso el que llama al recurso [22].

4.4. Ataques de denegación de servicio

Un tipo de ataque bastante conocido es el llamado ataque por denegación de servicio, el cual consiste en que el atacante lance una serie de peticiones de forma masiva contra un equipo de destino de tal manera que dicho equipo no sea capaz de procesar tantas peticiones y deje de prestar ningún tipo de servicio. Por poner un ejemplo imagine una cocina de un restaurante, el cocinero cada vez que le llega una petición se pone a preparar la comida hasta que la sirve; ahora imagine que le llegan miles de peticiones por segundo, algunas de estas peticiones será capaz de recordarlas y las procesará cuando acabe las actuales, otras sin embargo terminará por perderlas y jamás llegarán a ser procesadas. Exactamente eso es lo que ocurre con los equipos informáticos y los ataques DOS (Denial Of Service) o DDOS (Distributed Denial Of Service), dejar sin servicio a la página web de una compañía que vive de ello significa que va a tener pérdidas mientras dicho ataque se mantenga, además estos ataques están viendo aumentada su frecuencia [25] y aún más contra las empresas PyME [26] debido a que las grandes compañías están aprendiendo a protegerse. Debido a ello proliferan las compañías que ayudan a otras a protegerse contra este tipo de ataques, pero a un precio entre dos mil y diez mil dólares al mes, lo cual es un precio bastante alto [26].

La computación en la nube debería de ser una solución bastante fiable contra este tipo de ataques, debido a que cuando alguien hace una petición de cualquier tipo contra un servicio alojado en la nube, esta petición pasa por todo tipo de swiches, routers y firewalls hasta llegar a nuestro servidor, por lo que las compañías que proveen dicho servicio deberían de poner todo tipo de recursos a disposición del usuario para que no lleguen a pasar este tipo de ataques. Y realmente esto ocurre, pero no completamente, se han encontrado casos como `https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/` en los que los proveedores de soluciones de computación en la nube cobran grandes cantidades de dinero a sus clientes cuando sufren un ataque de denegación de servicio y se perpetúa en el tiempo. ¿Cuál es la razón por la que esto ocurra? Simple, los proveedores de computación en la nube cobran por el uso de sus infraestructuras y mientras el ataque no sea lo suficientemente potente para afectar a las mismas no van a poner todos los recursos posibles dado que eso les costaría dinero a ellos y, aunque ofrecen unos servicios mínimos de protección [27] no va a estar garantizada la misma, pero no todo está perdido, como se verá en el siguiente capítulo la tienda de Azure nos ofrece la instalación de firewalls avanzados para proteger nuestra red, al igual que Amazon la causante de la noticia hemos visto en este párrafo. Además, ambos proveedores ponen al servicio del cliente firewalls de las mismas compañías como puede ser el de cisco `https://aws.amazon.com/marketplace/pp/B01DCZSQY6`. Sin embargo, esta situación no es demasiado extraña, en entornos On premise cuando hablamos de securificar nuestro entorno para evitar ataques DDOS a nivel de infraestructura instalamos Firewalls los cuales nos pueden proteger en cierta medida y, si queremos ir más allá debemos de instalar un firewall de la siguiente generación (Next Generation FireWall), que a diferencia de los firewalls tradicionales de toda la vida que solo escanean IP y puertos de origen y destino, examinan los paquetes que atraviesan el NGFW lo cual permite protegernos de un mayor número de amenazas, incluso de un ataque de denegación de servicio [28] contra la infraestructura, uno de estos servicios como el de barracuda `https://www.barracuda.com/purchase` puede costar para una pequeña empresa unos seis mil euros al año según comerciales de la misma compañía, me costaría hacer el cálculo de lo que les costaría a las compañías proveedoras de *cloud computing* el coste de configurar firewalls para todos sus clientes sobre todo, teniendo en cuenta que son capaces de ofrecer máquinas virtuales

por 15 euros al mes. Una vez hablado de los NGFW que sirven para proteger la infraestructura podemos hablar de los 'Web Application Firewall' (WAF) que es otro tipo de Firewall avanzado que podemos instalar en servicios de *cloud computing*. Este tipo de Firewall es necesario debido a que los Firewall a nivel de infraestructura no son capaces de examinar el tráfico cifrado como el https, por lo que si alguna petición malintencionada llega al servidor de manera cifrada afectará al mismo. Una vez más Azure nos ofrece varios tipos de WAF de los cuales el de barracuda fue el primero en incorporarse a la tienda de Azure por lo que está más integrado que el resto, por ejemplo puede protegernos de todos los ataques del top10 de OWASp (De los que se hablan en el siguiente capítulo) y además evita que desde dentro de nuestra organización se puedan publicar datos confidenciales el coste de este servicio según el mismo comercial contactado en el párrafo anterior puede ser de tres mil euros al año.

Protegernos es caro, muy caro, pero el problema radica en que atacar sale barato, muy barato. Estamos hablando de que un nivel alto de protección mediante Firewalls de alto nivel nos sale a casi diez mil euros al año mientras que contratar en la Deep Web un servicio de DDOS sale a cuarenta euros la hora [29]. Como se ve en el siguiente capítulo podemos mejorar la seguridad de nuestras aplicaciones web haciendo uso de la computación en la nube, sin embargo alojar una aplicación en la nube y no protegerla lo suficiente puede tener costes muy elevados, aunque como cada empresa es diferente, en un escenario en el que la página web sea el pilar central de los ingresos de la compañía, lo más normal es configurar un NGFW y un WAF en su entorno On Premise o en la nube por lo que en mi opinión es en este caso cuando si compensa tener la web alojada en la nube, dado que dicha empresa necesita que su web se encuentre disponible el mayor tiempo posible del tiempo. Sin embargo existe otra opción si el hecho de tener la aplicación operativa el máximo tiempo necesario no es imprescindible, dicha opción sería apagar el servicio que esté siendo atacado, pero ¿Cómo podemos llevar esto a cabo? Creando una alerta sobre dicha aplicación que lleve a cabo la acción de apagado cuando se sobrepase un máximo de peticiones sobre ésta. Podemos ver cómo realizar esta acción en el anexo 'Tercer Escenario' pero previamente necesitamos tener al menos una de las aplicaciones creadas en el segundo escenario.

4.4.1. Analisis de coste de un DDOS en Azure

Una botnet es un entramado de equipos controlado con ciberdelincuente con mayor o menor tamaño, si lanzamos peticiones Http contra un servidor como hemos dicho podemos llegar a tirarlo, pero si no nos protegemos en Azure ¿Cual es el coste? Pongamos una botnet de 1000 equipos lanzando diez peticiones http a nuestro servidor por segundo. Una petición http puede constar de 2KB como máximo en exploradores como IE [30]. Esto hace un total de 864000 peticiones por equipo al día, 864000000 peticiones de toda la botnet. Como hemos dicho cada peticione puede constar de 2KB, 1728000000KB diarios en peticiones, que son 1'7 TB al día. Siguiendo la tabla de precios de Azure para el uso de ancho de banda en `https://azure.microsoft.com/es-es/pricing/details/bandwidth/` podemos determinar que este ataque tendría un coste de 4570 euros al mes.

4.5. Cumplimiento y normativa

El último tema de este trabajo tratará sobre la legalidad, un tema que no podemos perder de vista. Cuando una compañía española alberga datos de carácter personal, dichos datos están sujetos a la Ley Orgánica de Protección de Datos [31]. Dicha ley hace una mención a la seguridad de estos datos en el artículo nueve de la misma:

- 'El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los

datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.'

- 'No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.'
- 'Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley (el artículo 7 hace referencia a los datos de tipo ideológico, racial, étnico... y prohíbe).'

El hecho que una compañía almacene datos personales de sus empleados, clientes o terceras personas no la exime de tener que cumplir con las obligaciones a las que se refiere. La agencia española de protección de datos ha creado una guía para clientes que contraten servicios de *cloud computing*, en la que se detalla este hecho, la compañía contratante será la responsable en caso de que se vulnere dicha ley. Es más, seguirá siendo responsable aunque incorpore una cláusula en el contrato que indique que la empresa que alberga los datos se hace responsable [32].

También existe un problema sobre la ubicación de estos datos. Si contratamos un proveedor con su centro de datos en la Unión Europea, Islandia, Liechtenstein o Noruega, no tendremos ningún problema en cuanto a la ubicación de los datos se refiere, ya que no se considera que exista transferencia de datos. En particular, con Azure no tendremos ningún problema en cuanto a la ubicación de los datos, ya que tiene centros en Irlanda, Países Bajos, Frankfurt, Magdeburgo, Cardifg y Londres [33]. Con AWS tampoco tenemos problemas ya que tiene centros en Frankfurt, Irlanda y Londres [34]. En caso de que alojemos nuestros datos en un centro no situado en los países anteriores debemos de tener en cuenta que para seguir cumpliendo la ley, el proveedor debe proporcionar garantías jurídicas apropiadas, ya que se considera que existe transferencia internacional de datos. En dicho caso tenemos que mirar si la agencia Española provee dichas garantías, por ejemplo Azure tiene dicha certificación para todas sus sedes, mientras que por ejemplo AWS no dispone de dichas garantías en alguno de sus centros de datos y, en caso de guardar datos personales en su centro de Bombay estaremos inclumpiendo la LOPD [35] [36].

Una vez sepamos que podemos almacenar los datos, tenemos que distinguir un nivel de seguridad dependiendo del tipo de dato que vamos a almacenar [37]. En resumidas cuentas existen:

- Alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual; contengan o se refieran a datos recabados para fines policiales, sin consentimiento de los afectados; contengan datos derivados de actos de violencia de género.
- Medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales.
- Bajo: Resto de ficheros

Además, se nos tiene que garantizar una serie de condiciones a la hora de acceder a los datos, ya que estamos haciendo uso de las redes de comunicaciones [38]. La seguridad que vimos en el primer capítulo sobre como Azure protege datos y otras garantías más es suficiente para garantizar estos dos últimos puntos relativos a la seguridad de los datos [39].

Un punto más a tener en cuenta es que el proveedor en la nube tiene que garantizar la confidencialidad de los datos. Al respecto podemos mirar si el proveedor cumple con la ISO/IEC

27018 que garantiza la protección de datos en *cloud*, certificado que por ejemplo cumplen AWS y Azure. Siempre debemos buscar en información acerca de cómo el proveedor de servicios garantiza tanto confidencialidad como transparencia.

Podemos examinar las certificaciones de seguridad de las dos grandes empresas que en la actualidad tratan con la nube.

- Azure: `https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings`
- Azure Web Services: `https://aws.amazon.com/es/compliance/`

Como podemos observar, ambas plataformas se esfuerzan por aumentar la seguridad de su plataforma y cumplen muchos estándares que serían difíciles de alcanzar y renovar anualmente para cualquier pequeña o mediana empresa.

4.5.1. Regulación General de protección de datos

En 2016 entró en vigor una nueva legislación de protección de datos a nivel europeo, esta legislación es como la Ley Orgánica de Protección de Datos en España, a mayor grado. Lo que trae como consecuencia que dicha ley quede en un segundo plano, ya que lo que hace es aunar todas las leyes previamente existentes en los países miembros de la Unión en una única ley. Incumplir dichas normativas puede tener consecuencias de hasta veinte millones de euros o un cuatro por ciento de los ingresos anuales [40]. Dado que los proveedores de computación en la nube construyen sus soluciones de cara a cumplir con todas las normativas vigentes y, que tienen más recursos para conseguirlo será más fácil para una compañía que contrate sus servicios con dichas empresas cumplir con todas las normativas [41] [42]. El surgimiento de esta ley representa que debemos de cumplir con la misma. Además con las exigencias que trae consigo la LOPD que hemos visto en el apartado anterior, hasta que dicha regulación se aplique el 25 de mayo de 2018 hay que seguir cumpliendo con la LOPD [43].

La novedades más importantes respecto a la LOPD española las podemos encontrar en la guía de la Agencia Española de Protección de Datos [44].

- Derecho de acceso:
  - Antes: Debían facilitarse todos los datos de base del afectado,pero no copias o documentos (excepto en el caso de la historia clínica).
  - Ahora: Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento

  Lo que significa que en caso de que se nos requiera documentación por motivos legales podemos conservar los datos.
- Derecho al olvido: Tenemos derecho a eliminar completamente todos nuestros datos de la nube sin que quede rastro de los mismos.
- Medidas de seguridad: La RGPD pide que las medidas de seguridad a la hora de proteger los datos sean mayores que anteriormente .
- Violación de los datos: En caso de que un ciberdelincuente consiga vulnerar la seguridad y se haga con los datos, la empresa debe comunicarlo a la autoridad de protección de datos pertinente, lo que significa que si nuestros datos se ven vulnerados la compañía tendrá conocimiento de ello. Además en un plazo de 72 horas, por lo que podremos actuar en consecuencia si ello ocurriese.
- Se han endurecido los requisitos a la hora de transferir datos internacionalmente.

5

Conclusiones y trabajo futuro

Sin lugar a dudas, la nube es el presente de muchas empresas tecnológicas, y eso está llevando a que los usuarios la disfruten en multitud de aplicaciones de uso cotidiano. Las grandes empresas tecnológicas están pujando fuerte por tener plataformas comerciales que puedan usar todas las empresas, ya sean grandes, medianas o pequeñas. Son las dos últimas las que pueden encontrar de mayor utilidad este trabajo ya que hemos tratado diversos aspectos que muchas de ellas necesitarán. Una empresa de menos de 10 empleados puede utilizar una aplicación de tipo Software as a Service despreocupándose totalmente de la seguridad de la infraestructura que está por debajo del Software. Además puede utilizar Azure AD para autenticar de manera segura a sus empleados o crear una aplicación B2C en la que no se tendrá que preocupar de la seguridad relativa a la autenticación de los usuarios. Las empresas medianas, que son las que mayor interés tienen en tener máquinas virtuales, podrán tenerlas sin tener en cuenta la seguridad de las redes que las envuelven y se verán más beneficiadas del almacenamiento de datos en la nube. Tendrán recomendaciones de seguridad sobre sus entornos gracias a herramientas como Advisor. Pero todo esto tiene un requisito fundamental **confianza**, la confianza es la clave en la nube. Tenemos que depositar todas nuestras esperanzas en que el proveedor en el que tenemos software, plataforma o infraestructura no haga mal uso de nuestros datos y su entorno sea más seguro que el que nosotros podamos conseguir con los recursos económicos y humanos de los que disponemos. Se han visto además consideraciones a tener en cuenta a la hora de utilizar servicios en la nube, hemos de mirar que el proveedor en la nube cumpla nuestras necesidades y, que al mismo tiempo cumpla la ley, ya que de lo contrario utilizar dichos servicios puede salirnos muy caro. Como opinión personal he de decir que, aunque la documentación que he tenido que leer por parte de Microsoft era completa, no era todo lo completa que cabía desear, muchas veces aportan guías muy completas, pero se dejan pequeños detalles como puede ser publicar la aplicación en Azure y no simplemente crear el proyecto de manera local. También he de decir que en la comunidad de 'Server Fault' y por Twitter siempre hay profesionales de la compañía dispuestos a ayudar con pequeñas dudas, lo cual es de gran ayuda para profesionales que se empiezan a integrar en dicho mundo. Aunque en este trabajo se han buscado soluciones que aumenten la seguridad en varios servicios que utilizan las PYME, aún quedan varios servicios que no se han podido estudiar. Éstos pueden ser dos pilares tan fundamentales como las bases de datos o un servidor de correo. Azure ofrece soluciones de bases de datos SQL como se ha podido ver en el segundo escenario, pero no ofrece ninguna para albergar un servicio de correo al margen de una máquina virtual.

En un futuro me gustaría trabajar con la plataforma en la nube de Amazon, ya que hoy en día tiene una cuota de mercado muy superior al resto de sus competidores y dispone de tecnologías muy semejantes a las que se han tratado en este documento. Además, me gustaría tratar otras tecnologías de Azure orientadas a la seguridad como pueden ser **Key Vault** como servicio de almacenamiento de claves criptográficas, **Azure WAF** como firewall de aplicaciones o **Azure Active Directory Domain Services** una plataforma SaaS de Active Directory. También sería interesante expandir el proyecto utilizando las nuevas tecnologías que van apareciendo ya que, cada pocos meses las compañías en la nube incorporan nuevos servicios. Por ejemplo, mientras desarrollaba el presente documento una nueva tecnología denominada 'Bussiness to Bussiness' salió a la luz por parte de Azure, dicha tecnología permite crear aplicaciones en las cuales la autenticación se realiza a través de los servicios de Azure Active Directory de dos compañías distintas. Lo cual permite ahorrar el paso de dar de alta en nuestro directorio a usuarios de otra compañía como se venía haciendo hasta ahora. Otro punto más a desarrollar es la parte de cómo se confecciona el uso de las redes en las plataformas en la nube. En este trabajo se han creado máquinas virtuales y se les ha asignado una subred, por lo que las máquinas tenían comunicación entre sí, pero si tenemos varios servidores hay que confeccionar las redes en las que se alojan de manera segura, de tal manera que todos los servicios se encuentren aislados entre sí. Además hay que profundizar en todas estas tecnologías ya que, únicamente se ha dado una pincelada sobre cada una de ellas, ahondar más en dichas tecnologías permitirá aumentar aún más la seguridad de los servicios que proporciona nuestra empresa, ya sea de cara a clientes o a empleados. El problema de que existan tantas tecnologías es que es muy difícil controlas todas a la perfección y para ello se necesitaría más personal que maneje los sistemas, lo cual es algo que una PYME siempre intenta evitar, ya que ese es uno de los motivos que hemos considerado para migrar a la nube. Por último sería interesante analizar las soluciones de seguridad que ofrece la nube para dispositivos IoT (Internet de las cosas). Dicha tecnología usa montones de datos de todo tipo de dispositivos y, si dichos datos no se manejan ni se envían de forma segura puede tener graves consecuencias.

Glosario de acrónimos

- **AAD**: Azure Active Directory: Servicio SaaS de Active Directory en Azure.
- **AWS**: Amazon Web Services: Plataforma que ofrece la compañía Amazon que ofrece servicios de computación en la nube....
- **B2C**: Bussiness to Consumer: Aplicación que crea una compañía para ser consumida por el público en general.
- **Backend**: Zona de administración de una aplicación, sólo accesible para administradores.
- **DDOS**: Distributed Denial Of Service: Tipo de ciberataque que consiste en realizar multitud de peticiones ilegítimas a un servidor para que no sea capaz de procesar ningún tipo de petición legítima.
- **Cloud**: Nube, aplicación, dato, sistema que no se encuentra alojada en el sistema
- **IaaS**: Infraestructura como servicio, el concepto es simple, se nos provee una máquina virtual que estará alojada en la nube, el usuario se conectará con escritorio remoto y ofrece las mismas posibilidades que una máquina virtual
- **MFA**: Multi-Factor Authentification, Autenticación de usuarios en varios pasos, será la combinación de una contraseña, algo que se tiene (dispositivo) y algo que se es (Una huella dactilar)
- **On Premise**: Aplicación, dato, sistema que se encuentra alojado en tu sistema
- **PaaS**: Plataforma como servicio, evolución de Iaas, el usuario gestiona y programa la aplicación, el proveedor nos proporciona la infraestructura, haciendo transparentes las capas inferiores, ejemplos pueden ser una aplicación o API web
- **PyME**: Pequeña o mediana empresa; dícese de la empresa que tiene menos de doscientos cincuenta empleados y que tiene un volumen de negocio menor a cincuenta millones de euros [45]
- **SaaS**: Software como servicio, evolución de IaaS, utilizamos software existente de otro fabricante el cual podremos modificar y gestionar, un ejemplo en la tienda de Azure es Wordpress, un famoso gestor de contenidos web...
- **VS**: Visual Studio: IDE de programación de Microsoft, permite desarrollar en entornos como python, ASP, javascrip....

Bibliografía

[1] Ministerio de industria energía y turismo. Estadísticas pyme. http://www.ipyme.org/publicaciones/estadisticas-pyme-2015.pdf. Revisado el 22/06/2017.

[2] Laurent Giret. Microsoftś azure making gains in business use, survey shows. https://www.onmsft.com/news/microsofts-azure-making-gains-in-business-use-survey-shows. Revisado el 22/06/2017.

[3] Microsoft. Azure products. https://azure.microsoft.com/en-us/services/. Revisado el 22/06/2017.

[4] Amazon. Productos de la nube. https://aws.amazon.com/es/products/. Revisado el 22/06/2017.

[5] Google. Google cloud platform solutions. https://cloud.google.com/solutions/. Revisado el 22/06/2017.

[6] Amazon. Aws directory service. https://aws.amazon.com/es/directoryservice/faqs/. Revisado el 22/06/2017.

[7] Microsoft. Azure active directory. https://docs.microsoft.com/es-es/azure/active-directory/active-directory-whatis. Revisado el 22/06/2017.

[8] Microsoft. What is application access and single sign-on with azure active directory? https://docs.microsoft.com/en-us/azure/active-directory/active-directory-appssoaccess-whatis. Revisado el 22/06/2017.

[9] Microsoft. Azure active directory identity protection. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection. Revisado el 22/06/2017.

[10] Florin Bodnarescu. Microsoft becomes the first cloud provider to offer gdpr contractual commitments publicly. https://www.neowin.net/news/microsoft-becomes-the-first-cloud-provider-to-offer-gdpr-contractual-commitments-publicly. Revisado el 22/06/2017.

[11] Wikileaks. Vault 7: Cia hacking tools revealed. https://wikileaks.org/ciav7p1/. Revisado el 22/06/2017.

[12] Rosa Jiménez Cano. Apple niega al fbi acceso al iphone del tirador de san bernardino. `http://internacional.elpais.com/internacional/2016/02/17/actualidad/1455702891_642434.html`. Revisado el 22/06/2017.

[13] Lisa Vaas. Microsoft to host data in germany to evade us spying. https://nakedsecurity.sophos.com/2015/11/12/microsoft-to-host-data-in-germany-to-evade-us-spying/. Revisado el 22/06/2017.

[14] Microsoft. What problems does azure rms solve. https://docs.microsoft.com/en-us/information-protection/understand-explore/azure-rms-problems-it-solves. Revisado el 22/06/2017.

[15] Microsoft. What is azure information protection? https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection. Revisado el 22/06/2017.

[16] Microsoft. Precios azure storage. https://azure.microsoft.com/es-es/pricing/details/storage/blobs/. Revisado el 22/06/2017.

[17] Microsoft. Cifrado del servicio almacenamiento de azure para datos en reposo. https://docs.microsoft.com/es-es/azure/storage/storage-service-encryption. Revisado el 22/06/2017.

[18] Microsoft. Cifrado del lado de cliente y almacén de claves de azure para el almacenamiento de microsoft azure. `https://docs.microsoft.com/es-es/azure/storage/storage-client-side-encryption#a-namebest-practicesaprácticas-recomendadas`. Revisado el 22/06/2017.

[19] Microsoft. Tamaños de las máquinas virtuales windows en azure. https://docs.microsoft.com/es-es/azure/virtual-machines/virtual-machines-windows-sizes. Revisado el 22/06/2017.

[20] Microsoft. Serie de máquinas virtuales. https://azure.microsoft.com/es-es/pricing/details/virtual-machines/series/. Revisado el 22/06/2017.

[21] Microsoft. Cuentas de blob storage. https://azure.microsoft.com/es-es/pricing/details/storage/blobs/. Revisado el 22/06/2017.

[22] Microsoft. Getting started with microsoft azure security. https://docs.microsoft.com/es-es/azure/security/azure-security-getting-started#a-namevirtualizationavirtualización. Revisado el 22/06/2017.

[23] Chema Alonso. Emular una máquina virtual y evitar infección de malware. http://www.elladodelmal.com/2014/03/emular-una-maquina-virtual-y-evitar.html. Revisado el 22/06/2017.

[24] Ruby B. Lee Diego Perez-Botero, Jakub Szefer. Characterizing hypervisor vulnerabilities in cloud computing servers. http://dl.acm.org/citation.cfm?id=2484406. Revisado el 22/06/2017.

[25] Verisign. Q4 2016 ddos trends report: 167 percent increase in average peak attack size from 2015 to 2016. https://blog.verisign.com/security/q4-2016-ddos-trends-report-167-percent-increase-average-peak-attack-size/. Revisado el 22/06/2017.

[26] John E Dunn. Uk smes and ddos attacks - a survival guide for defending smaller organisations. http://www.techworld.com/security/uk-smes-ddos-attacks-survival-guide-for-defending-smaller-organisations-3625407/3/. Revisado el 22/06/2017.

[27] Microsoft. Microsoft cloud services and network security. https://docs.microsoft.com/en-us/azure/best-practices-network-security. Revisado el 22/06/2017.

[28] Check Point. Next generation threat prevention. https://www.checkpoint.com/products-solutions/threat-prevention/. Revisado el 22/06/2017.

[29] Pierluigi Paganini. 38$ an hour is the cost of destructive ddos attacks. http://securityaffairs.co/wordpress/37819/cyber-crime/cost-of-ddos-attacks.html. Revisado el 22/06/2017.

[30] Microsoft. Maximum url length is 2,083 characters in internet explorer. https://support.microsoft.com/en-us/help/208427/maximum-url-length-is-2,083-characters-in-internet-explorer. Revisado el 22/06/2017.

[31] Gobierno de España. Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. Revisado el 20/06/2017.

[32] Agencia Española de Protección de datos. Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud Revisado el 21/06/2017.

[33] Microsoft. Regiones azure. https://azure.microsoft.com/es-es/regions/. Revisado el 21/06/2017.

[34] Amazon. Infraestructura global de aws. https://aws.amazon.com/es/about-aws/global-infrastructure/. Revisado el 21/06/2017.

[35] Microsoft news center. La agencia española de protección de datos (aepd) confirma las garantías de los servicios corporativos de microsoft en la nube para la exportación de datos. https://news.microsoft.com/es-es/2014/06/06/aepd-servicios-cloud-microsoft/. Revisado el 21/06/2017.

[36] Amazon. Transferencias internacionales de datos amazon. https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php. Revisado el 21/06/2017.

[37] Agencia Española de Protección de Datos. Clasificación por niveles de las medidas de seguridad requeridas a ficheros y tratamientos. https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=1120. Revisado el 21/06/2017.

[38] Agencia Española de Protección de Datos. Condiciones para el acceso a datos personales a través de redes de comunicaciones. https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00004. Revisado el 21/06/2017.

[39] Microsoft. Como microsoft protege los datos. https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx. Revisado el 21/06/2017.

[40] Dr Kuan Hon. Gdpr: potential fines for data security breaches more severe for data controllers than processors, says expert. https://www.out-law.com/en/articles/2016/may/gdpr-potential-fines-for-data-security-breaches-more-severe-for-data-controllers-than-processors-says-expert/. Revisado el 22/06/2017.

[41] Microsoft. Accelerate gdpr compliance with the microsoft cloud. https://www.microsoft.com/en-us/trustcenter/Privacy/GDPR. Revisado el 22/06/2017.

[42] Amazon. Aws and the general data protection regulation (gdpr). https://aws.amazon.com/es/blogs/security/aws-and-the-general-data-protection-regulation/. Revisado el 22/06/2017.

[43] Agencia Española de Protección de Datos. El reglamento de protección de datos en 12 preguntas. http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_0 ides-idphp.php. Revisado el 21/06/2017.

[44] Agencia Española de Protección de Datos. Guia del reglamento general de protección de datos para responsables de tratamiento. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf. Revisado el 21/06/2017.

[45] Gobierno de España. Definición de pyme en la ue. http://www.ipyme.org/es-ES/UnionEuropea/UnionEuropea/PoliticaEuropea/Marco/Paginas/NuevaDefinicionPYME.aspx". Revisado el 22/06/2017.

[46] psignoret. aad-sso-wordpress. https://github.com/psignoret/aad-sso-wordpress. Revisado el 22/06/2017.

A

Creación de cuenta y familiarización con Azure

A.0.1. Creación de una cuenta

Crear una cuenta en Azure es simple y además podemos crear una cuenta de prueba con una cantidad de crédito almacenado desde `https://azure.microsoft.com/es-es/free/`. Al crear dicha cuenta se nos pedirán datos básicos como nombre, dirección de correo, organización... Y dos que no lo son tanto. En primer lugar una tarjeta de crédito (No se cobra nada ni no se excede el crédito almacenado) y un domino. Dicho dominio es gratuito, aunque terminará en 'onmicrosoft.com', lo cual suele ser un problema para las compañías, ya que si tienen una página web o correo prefieren que se les conozca como usuario@organizacion.com a usuario@organizacion.onmicrosoft.com. Esto no es problema, ya que si tenemos nuestro propio dominio podremos utilizarlo más adelante en lugar del dominio 'onmicrosoft'.

A.0.2. Familiarización

Una vez tengamos nuestra cuenta creada, para acceder a la página de Microsoft Azure debemos acceder a https://portal.azure.com e iniciar sesión con nuestro usuario de correo electrónico con el que nos hemos registrado (Figura Portada Azure).

En el centro de la imagen podemos acceder a los recursos de ayuda o los más usados recientemente.

En el panel de la izquierda podemos observar botones para movernos a través de la aplicación, los más importantes son:

- Grupos de recursos: Desde aquí podemos ver los grupos de recursos que hemos generado. Un grupo de recursos es un contenedor, en él podemos almacenar, máquinas virtuales, redes, páginas web... ...
- SQL Database: Aquí se mostrarán todas las bases de datos SQL generadas, este tipo de bases de datos son las de Microsoft. Podemos agregar una nueva y gestionar las existentes. ...

- Máquinas virtuales: Desde aquí podemos crear, y gestionar diferentes máquinas virtuales prefabricadas, estas máquinas virtuales pueden tener sistemas operativos Microsoft, Linux, Red Hat... . . .
- Suscripciones: Pantalla de gestión de las suscripciones de Azure, desde aquí podremos ver de manera detallada el crédito restante de nuestra suscripción y en qué se ha consumido. . . .
- Azure Active Directory: Active Directory ofrecido como Saas, tiene una gran potencia, pero no nos ofrece todas las configuraciones que nos ofrece instalar Active Directory en una máquina. . . .
- Security Center: Pantalla desde donde nos aparecerán consejos y riesgos de seguridad de nuestros servicios en la nube. . . .
- Suscripciones: Aquí se detalla el gasto de nuestras suscripciones asociadas a la cuenta, ya que podemos tener más de una. Pero para una PyME no recomiendo tener varias suscripciones, ya que los recursos que creemos se asignan a una suscripción, y crear varías suscripciones hace más difícil la administración . . .

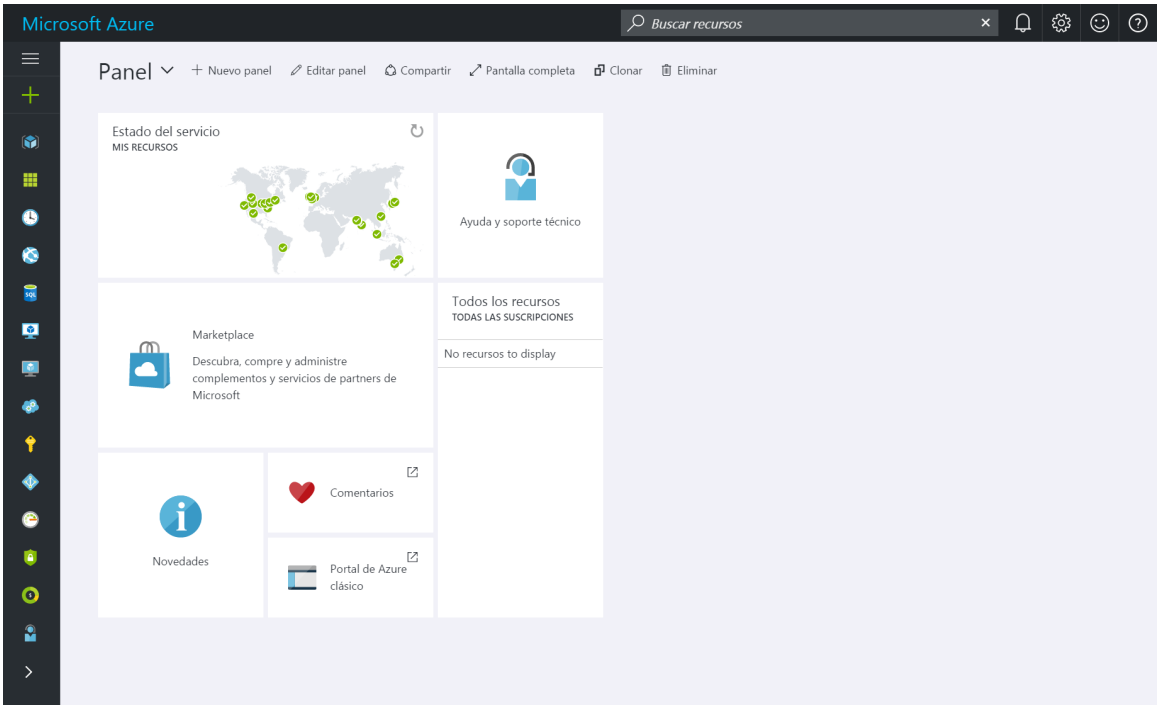


Figura A.1: Portada Azure

B

Creación del primer escenario

En este primer escenario vamos a crear todo el entorno de trabajo que utilizaremos en otro escenarios lo que incluye la creación de los usuarios y de un servicio Active Directory.

/sectionInstalación de Active Directory

/subsectionInstalación de Active Directory en máquinas virtuales en Azure

En esta sección vamos a crear un servidor Active Directory en una máquina virtual en Azure y crearemos otros equipos clientes para demostrar que funciona correctamente.

En primer lugar, montaremos el escenario en Azure:

Para crear nuestro servidor, en el portal de Azure, debemos dirigirnos al apartado máquinas virtuales, a continuación pulsaremos en agregar y buscaremos '*Windows Server 2016*' para buscar la versión más actualizada de Windows Server (Figura: Resultado de búsqueda 1).

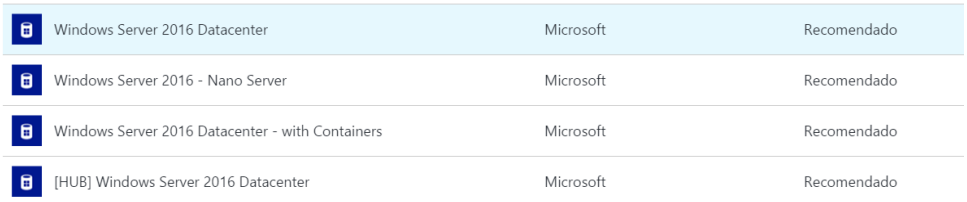


Figura B.1: Resultado de búsqueda 1

De todas las opciones que nos aparecen de momento nos interesa la primera de todas, ya que es el servidor con entorno gráfico y características básicas. El segundo únicamente tiene modo terminal, el tercero trae instalado Docker por defecto, lo cual no nos interesa para este escenario y el último para crear una granja de servidores.

Cuando hayamos elegido el servidor, crearemos un grupo de recursos de nombre Escenario1 y completaremos las configuraciones necesarias de nombre de usuario y contraseña a nuestro antojo. Elegiremos una máquina virtual barata, en mi caso 2 GB, un núcleo y HDD y dejaremos el resto de pasos por defecto.

De la misma manera vamos a crear un equipo con Windows 7 y Windows 10 en el mismo grupo de recursos.

A continuación, montaremos el mismo escenario en máquinas virtuales en un ordenador.

Al montar las máquinas virtuales en un grupo de recursos en Azure automáticamente estarán en la misma subred, por lo que no necesitamos ninguna configuración sobre la red, habilitando los paquetes ICMP desde el firewall de Windows, podremos hacer uso del comando Ping para comprobar este caso (Figura: Ping máquinas Azure 1).

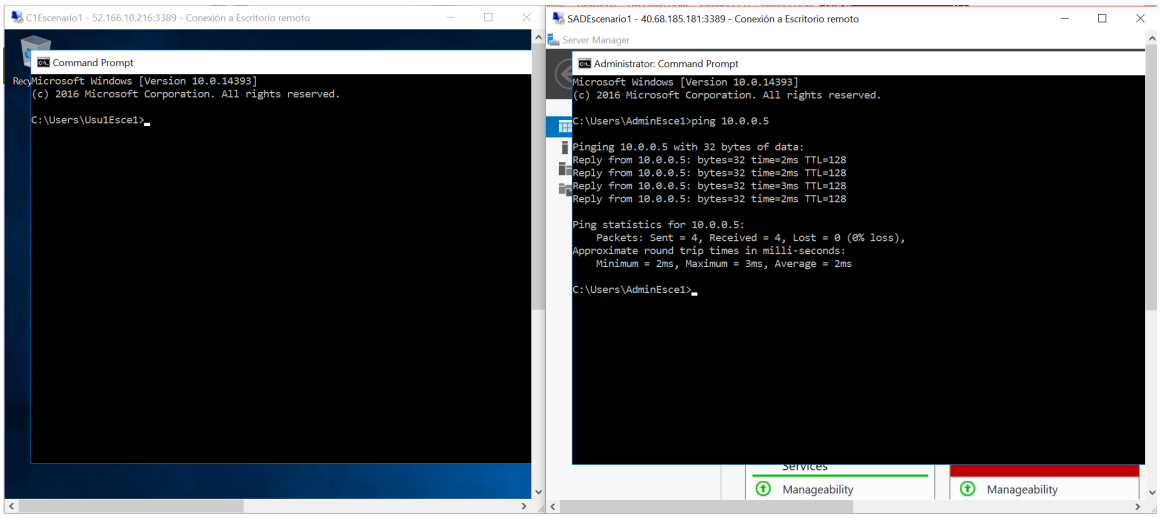


Figura B.2: Ping máquinas Azure 1

Ahora podemos pasar a la instalación de Active Directory en el servidor, lo haremos de manera guiada. Para ello en el administrador del servidor pulsaremos en añadir roles y características. El tipo de instalación será basado en roles ya que la instalación se realizará en este servidor. En la siguiente pantalla seleccionaremos el servidor en el que nos encontramos, en mi caso SADEscenario1.

En la siguiente pantalla se nos muestran todos los roles que podemos agregar al servidor, alguno de ellos los mostraremos en otros temas, pero el que nos concierne en este caso es: Active Directory Domain Services (Figura: Roles Servidor).

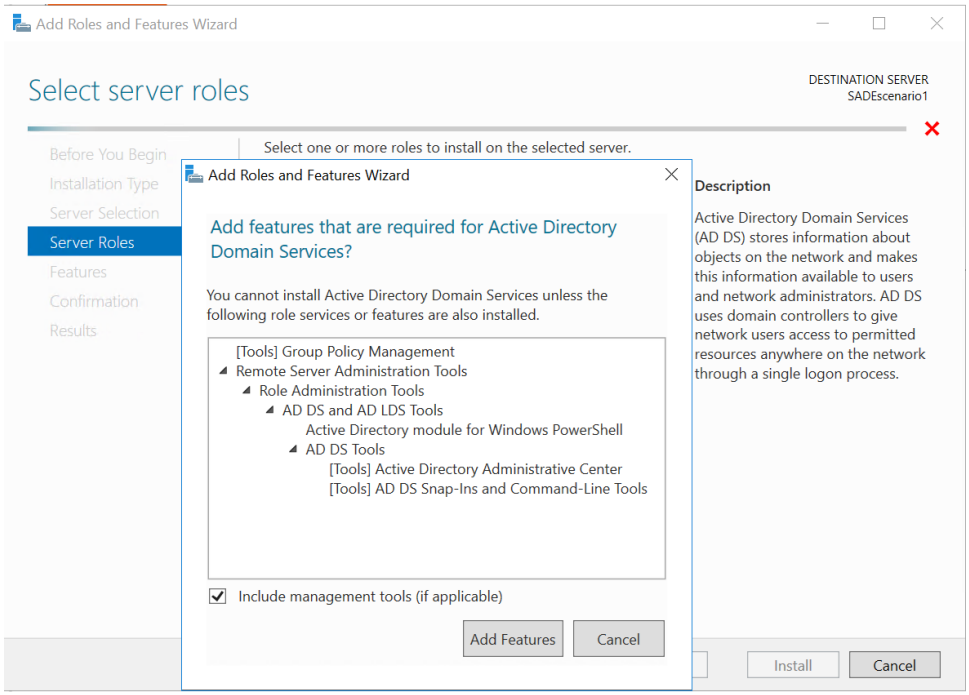


Figura B.3: Roles Servidor

Cuando le marcamos, nos aparece una ventana en la que se nos muestran otros servicios asociados a Active Directory que son necesarios para la instalación. De momento no necesitaremos instalar nada más y procederemos a finalizar la instalación. El proceso de instalación únicamente instala el programa de Active Directory, no crea un dominio ni lo une, eso se hará cuando finalice la instalación. Para unir o crear al dominio debemos de promover el equipo a controlador de dominio (Figura: Promover).

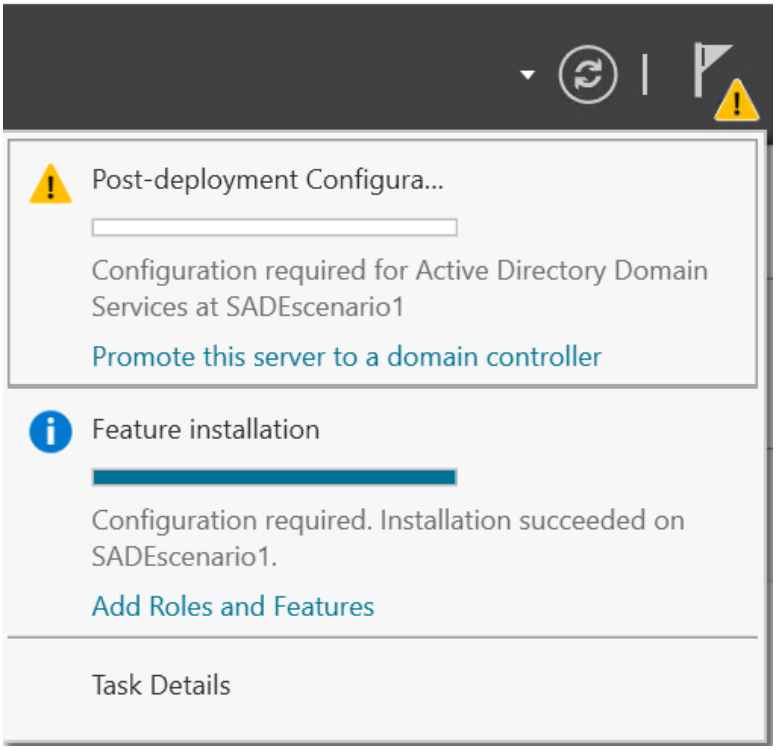


Figura B.4: Promover

Se nos abrirá un configurador que nos preguntará si unir el equipo a un dominio, crear un dominio en un bosque o si crear un nuevo bosque.

Un bosque es un conjunto de uno o varios dominios, todos los dominios de un bosque tendrán en común una parte del nombre, al igual que cuando hablamos de dominios y subdominios en Internet.

Unir un nuevo controlador a un dominio existente lo que hará será crear toda la configuración necesaria para que coexistan dos controladores de dominio en el mismo dominio replicando automáticamente la información que los servidores y respondiendo a las peticiones de los clientes.

Como aún no hemos creado ningún dominio no nos queda otra opción que crear nuestro propio bosque (Figura: Creación del dominio 1).

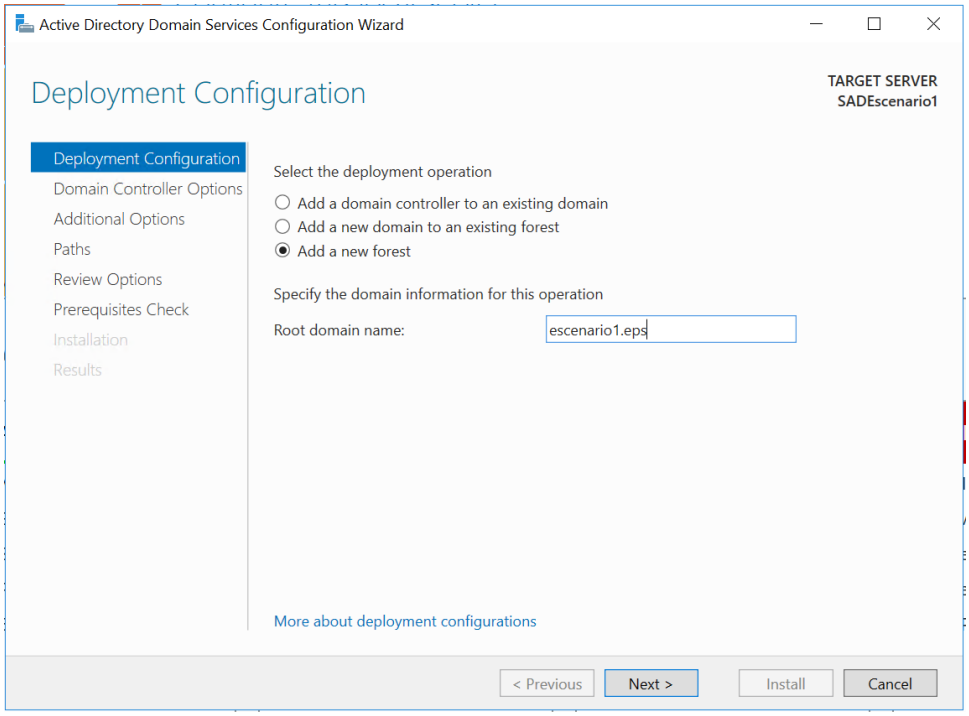


Figura B.5: Creación del dominio 1

El resto de la instalación es guiada y no se considera que se necesite de más ayuda para continuar, ya que únicamente se pide una contraseña de recuperación y si versiones anteriores de Windows Server podrán ser controladores de dominio. La instalación se llevará a cabo de manera automática, el equipo se reiniciará y cuando vuelva a estar disponible será parte de un dominio y controlador del mismo.

Una vez el equipo se reinicie dispondremos de todas las herramientas necesarias para la administración del directorio, para acceder a todas las herramientas administrativas desde el menú de inicio abrimos herramientas administrativas de Windows. Algunos útiles son:

- Dns: Nos permite ver toda la configuración DNS de los recursos de Active Directory y gestionar las configuraciones del servidor DNS. ...
- Centro de administración del Active Directory: Permite configurar, ver usuarios, grupos... de Active Directory. Básicamente contiene todas las herramientas en una sola. ...
- Usuarios y equipos de Active Directory: Permite la gestión y creación de usuarios, grupos y unidades organizativas. ...
- Dominios y confianza de Active Directory: Permite la gestión de todos los dominios que componen el bosque. ...

Para este escenario crearemos una ramificación cualquiera de usuarios y grupos, esto lo realizaremos desde la herramienta de usuarios y equipos (Figura: Usuarios escenario 1).

Una vez creado vamos a unir uno de los equipos clientes al dominio. Para ello debemos configurar en dicho equipo que uno de los servidores DNS del cliente va a ser el equipo con Active Directory. Una configurado el DNS debemos comprobar que se puede resolver el nombre del dominio, para ello efectuamos un ping al equipo servidor por su nombre de dominio (Figura: Ping DNS Servidor 1).

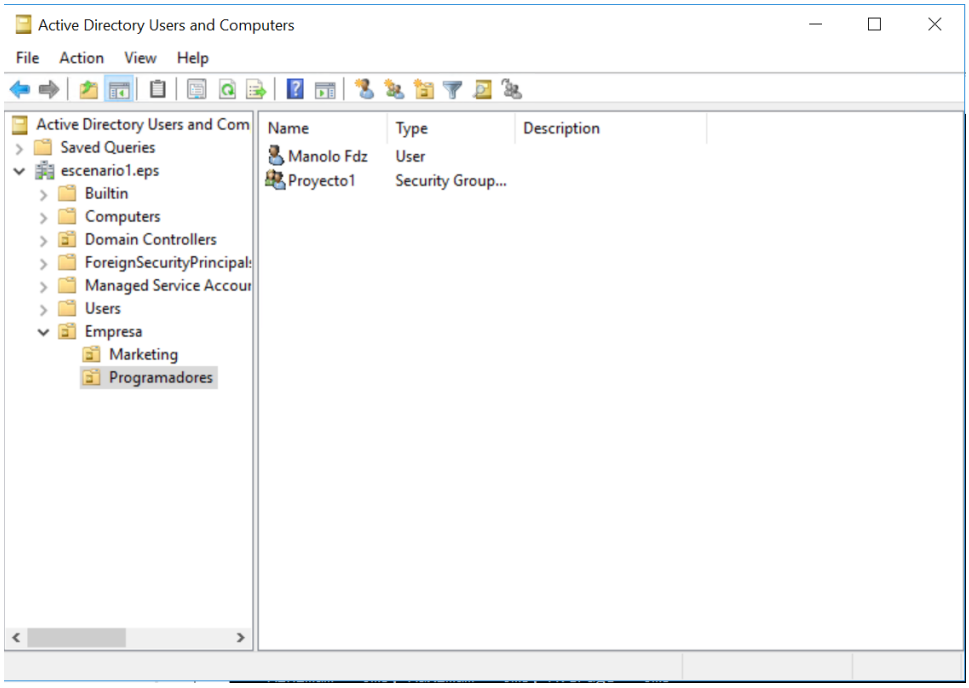


Figura B.6: Usuarios escenario 1

```
C:\Users\Usu1Esce1>ping SADEscenario1.escenario1.eps

Pinging SADEscenario1.escenario1.eps [10.0.0.7] with 32 bytes of data:
Reply from 10.0.0.7: bytes=32 time=8ms TTL=127
Reply from 10.0.0.7: bytes=32 time<1ms TTL=127
Reply from 10.0.0.7: bytes=32 time=8ms TTL=127
Reply from 10.0.0.7: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 4ms
```

Figura B.7: Ping DNS Servidor 1

A continuación, nos dirigimos a configuración del equipo, cuentas, unir el equipo a un dominio. A continuación, el equipo se reiniciará y ya será parte del dominio, cuando un equipo de la familia Windows forma parte de un dominio, se podrá iniciar sesión con usuario local o usuario de dominio al contrario que en equipos de la familia Linux, que sólo permiten el acceso con usuarios del dominio.

B.0.1. Creación de usuarios en Azure Active Directory

Automáticamente cuando se crea una cuenta en Azure se crea el servicio denominado Azure Active Directory, para ir al mismo debemos de ir al panel izquierdo y pulsar sobre el botón 'Azure Active Directory'. Antes de continuar, si pulsamos en el botón en la nueva barra que nos aparece 'Nombres de domino' podemos observar los nombres de dominio asociados, por defecto ya tendremos el que rellenamos al crear la cuenta (del tipo organizacion.onmicrosoft.com) pero esto significa que si creamos un usuario, su credenciales de acceso serán del tipo usuario@organizacion.onmicrosoft.com y preferiríamos algo del tipo usuario@organizacion.com. Yo para este documento no voy a crear ningún dominio porque tiene un coste, sin embargo mediante

el manual paso a paso de Vittorio Bertocci uno de los desarrolladores de AAD que se puede encontrar en su blog `http://www.cloudidentity.com/blog/2013/04/14/adding-a-custom-domain-to-your-wind` podremos comprar un dominio y asociarlo a nuestra cuenta.

Con nuestro dominio creado, vamos a crear a los usuarios que utilizaremos para autenticar a nuestros usuarios en las aplicaciones, para ello en el portal de Azure deberemos dirigirnos a la pestaña de Azure Active Directory, seleccionar usuarios y grupos, todos los usuarios, añadir y seleccionaremos sus datos como nombre, o grupo (creados a continuación). El rol de directorio por defecto será usuario, si le hacemos administrador global, dicho usuario tendrá acceso a la suscripción. Cuando creemos el usuario se nos mostrará una contraseña temporal que hemos de guardar y entregársela al usuario (En su primer inicio de sesión le será requerido que la modifique). El nombre con el que el usuario se autenticará en las aplicaciones estará compuesto por el nombre asignado y el dominio y, en mi caso tendrá la forma usuario@organizacion.onmicrosoft.com . Para crear los grupos, desde la pestaña de grupos de Azure Active Directory pulsaremos en nuevo, le daremos un nombre y guardaremos. Si queremos añadir un usuario a un grupo, podemos hacerlo desde la pestaña del miembros del grupo o en la pestaña grupos si nos dirigimos al usuario al que queremos introducir al grupo (Figura: Usuarios AAD escenario 1).

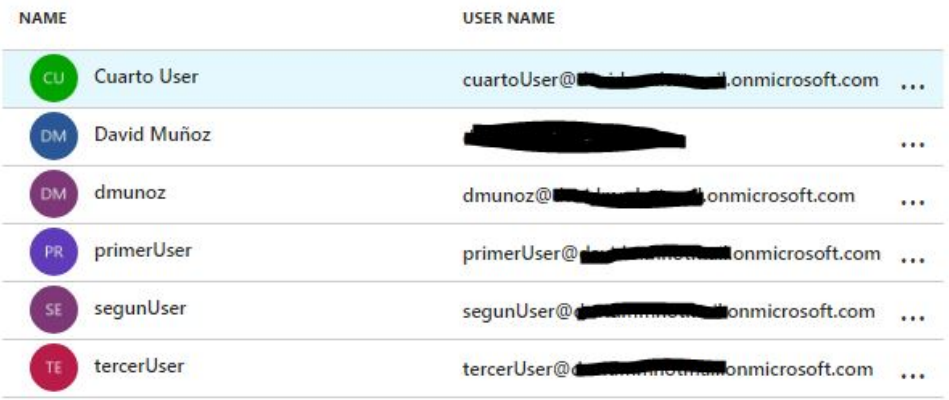


Figura B.8: Usuarios AAD escenario 1

Si queremos que un usuario externo utilice las aplicaciones de nuestra compañía (Como las web del segundo escenario), a la hora de dar de alta al usuario pincharíamos en 'Nuevo usuario invitado' en vez de 'Nuevo usuario'. Ésto nos permite añadir usuarios con cuentas tipo gmail, yahoo o cualquier otro dominio.

C

Creación del segundo escenario

C.1. Introducción y pasos necesarios

En este Anexo se crearán los proyectos Web sobre los que se realizan experimentos en el capítulo de seguridad de Azure; el objetivo de estos experimentos será autenticarnos contra ciertas aplicaciones de la forma más segura que nos ofrece Azure, esto es mediante la creación de usuarios en Azure y la autenticación contra un portal de Microsoft que será el que certificará que nos podemos autenticar contra dicha aplicación. Para la realización de este este escenario es necesario disponer de una cuenta de Azure y disponer de crédito en la misma, aunque puede llegar a realizarse sin disponer de crédito alguno utilizando los planes de servicio que ofrece Azure.

C.2. Creación de una web Wordpress con autenticación Single Sign On

En esta sección se va a detallar cómo se crearía una página web con el gestor de contenidos Wordpress y se realizará la autenticación de usuarios mediante Azure Active Directory. Wordpress es un blog de fácil creación y administración, dado que hay multitud de guías en Internet para gestionar este sitio web y se considera que este aspecto no debe estar cubierto por este documento, únicamente se explicarán los pasos para crear el sitio web y efectuar las configuraciones necesarias para crear un login seguro.

Debemos ir al portal Azure, a continuación en la pestaña de crear nuevo recurso buscaremos Wordpress y seleccionaremos la opción simple (Sin Linux). A la derecha nos aparecerá una descripción de lo que es Wordpress y pulsaremos el botón de crear.

Debemos de seleccionar el nombre de la app, la suscripción de la cuenta, el grupo de recursos y la base de datos 'Clear DB'. El plan app seleccionaremos el que mejor nos convenga. Existe un plan gratuito, pero no es recomendable ya hay que compartir infraestructura con otros usuarios. En mi caso elegiré un plan S1 que incluye:

50 GB de almacenamiento, dominio SSL (lo necesitamos en las siguientes aplicaciones), escalado automático a 10 instancias(Cuando tenemos mucho tráfico por un pico de trabajo se

replica el entorno en los servidores necesarios), backups diarios, 5 ranuras para la publicación de web apps y administradores de tráfico (Figura: Creación de servicio de app).

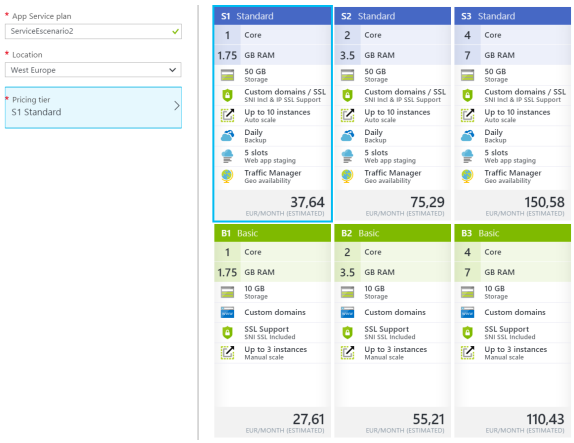


Figura C.1: Creación de servicio de app

`https://azure.microsoft.com/es-es/pricing/details/app-service/` Para finalizar aceptaremos los términos legales y pulsaremos en crear (Figura: Creación wordpress).

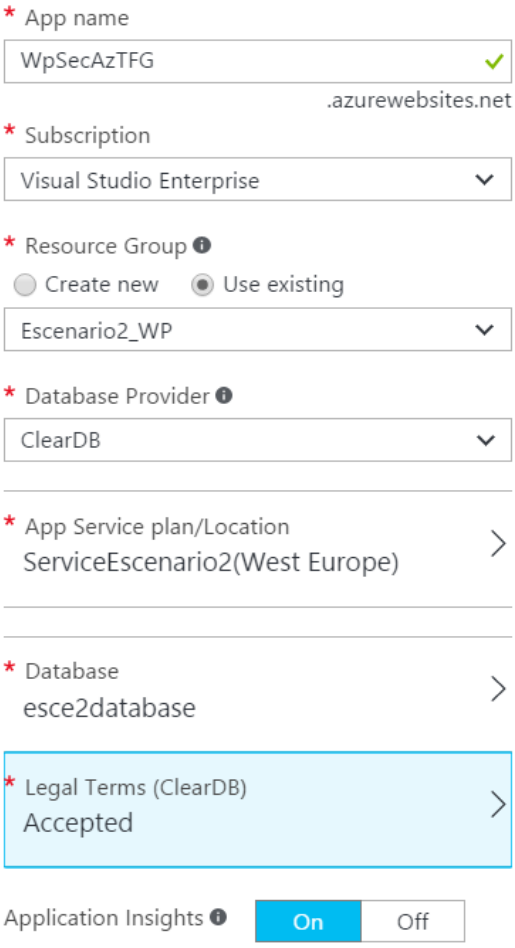


Figura C.2: Creación wordpress

Una vez hayamos realizado estas configuraciones empezará a desplegarse la aplicación web, y cuando termine (un par de minutos) ya estará accesible el portal de Wordpress desde cualquier navegador con conexión a Internet. Si el lector ha instalado en alguna ocasión un gestor de contenidos en una máquina, sabrá que una vez instalado el entorno hay realizar diversas configuraciones, como el idioma, contraseña de administrador... Pues una vez se ha instalado con Azure hay que realizar el mismo procedimiento. En primer lugar, se nos pedirá el idioma del portal, en la siguiente página se nos pedirá un título, nombre, contraseña y email. Este usuario de momento se guardará en la máquina en la que se instala Wordpress, aún no usaremos usuarios de Azure Active Directory.

La plantilla por defecto no deja acceder al portal a ningún usuario, y necesitamos que accedan usuarios, para ello vamos a cambiar el tema, para ello desde el portal de administración `paginaweb/wp-admin` en el escritorio pulsaremos en 'cambia tu tema por completo' y seleccionaremos cualquiera que tenga un login de usuarios, en mi caso 'Twenty Fourteen'. Si volvemos a acceder a la web veremos que ha cambiado el tema y que una de las opciones nos permite hacer login.

Hasta aquí es la instalación de cualquier portal de Wordpress, pero queremos ir más allá, queremos que los usuarios de nuestro AAD sean los únicos que pueden acceder a este portal como administradores y de una manera segura. [46] En primer lugar nos descargaremos el plugin para Wordpress desde `https://github.com/psignoret/aad-sso-wordpress` y lo instalaremos desde la consola de administración de Wordpress, en la pestaña de plugins pulsaremos en Añadir Plugin y seleccionaremos en archivo .zip que nos hemos descargado desde github, a continuación, pulsaremos en instalar, cuando termine de instalar (unos poco segundos) pulsaremos en activar.

Ahora debemos enlazar nuestro blog de Wordpress con AAD para permitir que los usuarios registrados en ADD puedan autenticarse contra el portal de Wordpress. Para ello, debemos de dirigirnos a la pestaña de Azure Active Directory en nuestro portal de Azure, a continuación, pulsaremos en el botón de portal clásico. En el portal clásico si no se nos ha redirigido a la pestaña de Azure Active Directory pulsaremos en ella y, a continuación, en 'Aplicaciones', agregar, aplicación que mi organización está desarrollando (Figura: Registro WP en ADD).

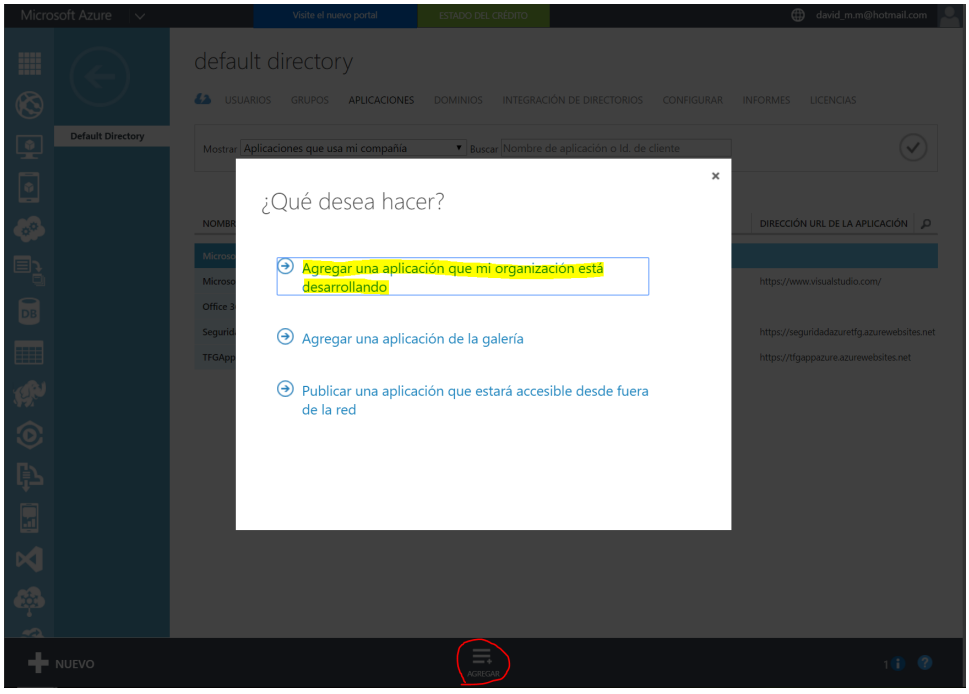


Figura C.3: Registro WP en ADD

En la siguiente pestaña, debemos de introducir el nombre con el que se identificará en ADD a la aplicación, no es necesario que sea el mismo que el de Web App, pero es recomendable para que sea fácilmente identificable, será una aplicación WEB, a continuación, introduciremos la url de inicio se sesión y la url de nuestra web. La url de inicio de sesión es la misma añadiendo '/wp-login.php' (Figura: Configurar URL APP AAD).

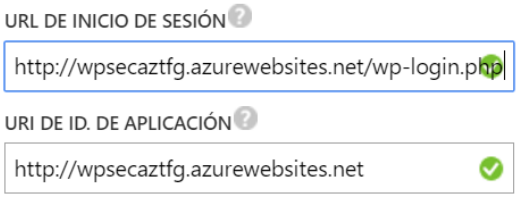


Figura C.4: Configurar URL APP AAD

Cuando este proceso finalice, debemos ir a la pestaña de configuración para dar permisos a la aplicación para leer los usuarios de AAD y generar una clave única que enlazará Wordpress con nuestro ADD.

Para ello, debemos de ir a la pestaña de configuración y en los permisos delegados para las aplicaciones seleccionar 'Read Directory Data' y 'Sign in and read user profile'. A continuación, en la sección de claves añadiremos una de uno o dos años, dependiendo de la frecuencia con la que queremos renovarlo. Esta clave se generará cuando se pulse el botón guardar, se mostrará en ese momento y nunca más se volverá a mostrar, así que hay que copiarla y guardarla en un lugar seguro (Figura: Permisos APP AAD).

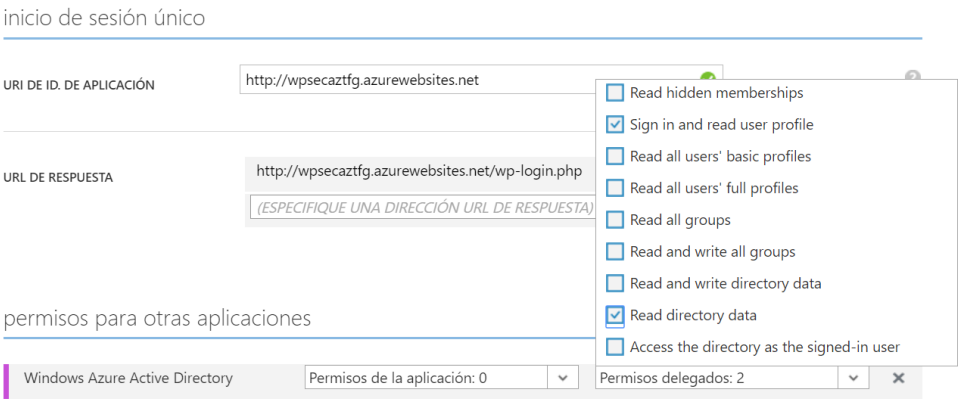


Figura C.5: Permisos APP AAD

El siguiente paso será configurar el plugin de ADD en Wordpress, para ello debemos de ir a la página de administración de Wordpress con el usuario administrador que configuramos al crear el sitio web, dirigirnos a Plugins -> Ajustes.

En esta pestaña en el cuadro de texto de 'Client ID' introduciremos el ID de cliente que aparecía en la pestaña de configuración de la aplicación de AAD que acabamos de configurar, y en client secret, la clave que apareció al guardar la configuración, también marcaremos las opciones 'Enable auto-provisioning' (Para que se puedan cargar los usuarios de ADD) y 'Enable auto-forward to Azure AD' (Para que sólo se puedan autenticar los usuarios de AAD. Finalmente pulsaremos en guardar cambios.

Ahora si nos dirigimos a la página de sesión de nuestro sitio web WordPress podremos observar que tenemos un nuevo enlace que nos permite autenticarnos mediante AAD (Figura:

Inicio Sesión WP).

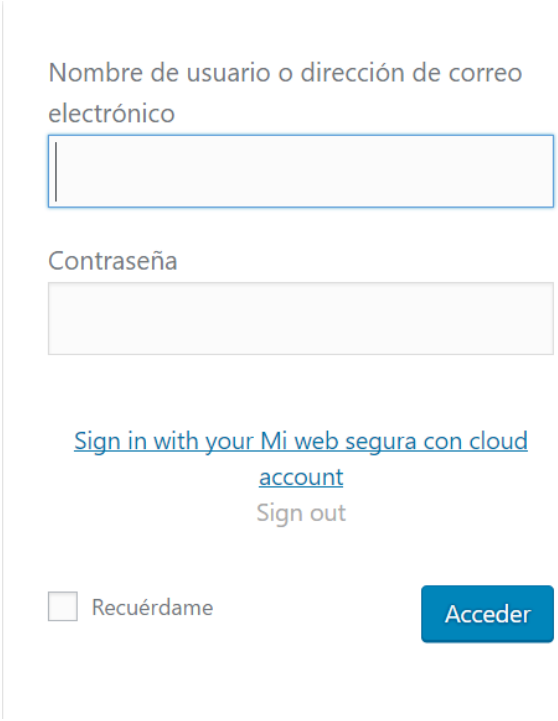


Figura C.6: Inicio Sesión WP

Si le pulsamos, nos veremos redirigidos a una página de inicio de sesión para cuentas Azure, en este punto es Microsoft el que nos garantiza la seguridad a la hora de entrar a nuestro sitio web. Si nos autenticamos, vemos que el usuario con el que hemos accedido no es administrador del sitio y no puede modificar el 'Backend'. Si queremos que uno de los usuarios de AAD tenga permisos de administración sobre el sitio, debemos entrar con el usuario administrador al 'Backend' del sitio, dirigirnos a la pestaña de usuarios y seleccionar el usuario al que queramos hacer administrado, y en el apartado de perfil le haremos administrador. (Para que un usuario aparezca entre los registrados se requiere un inicio de sesión en el sitio web, no se sincronizarán automáticamente todos los usuarios de nuestro sitio web). Por último, una última recomendación sería eliminar al usuario administrador que se creó durante la instalación del sitio y hacer que la única web de inicio de sesión sea la que está protegida por Azure, de esta manera no tendremos que protegernos contra inyecciones de código en la página tradicional de inicio de sesión de Wordpress. Para efectuar este paso, una vez tenemos un usuario de AAD con perfil de administrador, eliminaremos el usuario desde la pestaña de usuarios, a continuación, iremos a la pestaña de ajustes, Azure AD, y desde ahí seleccionaremos la opción 'Enable auto-forward to Azure AD' y guardaremos los cambios. Ahora si nos dirigimos a '/wp-login.php' observamos cómo somos automáticamente redirigidos a la web donde los únicos usuarios que pueden autenticarse son los de nuestro AAD. Además, si a dicho usuario le activamos la autenticación multi factor como se ve en el anexo 'Autenticación multi factor en el portal de Azure' se le pedirá que siempre que intente iniciar sesión lo haga con este método, lo cual es altamente recomendable para los administradores (Figura: Sesión WP Azure).

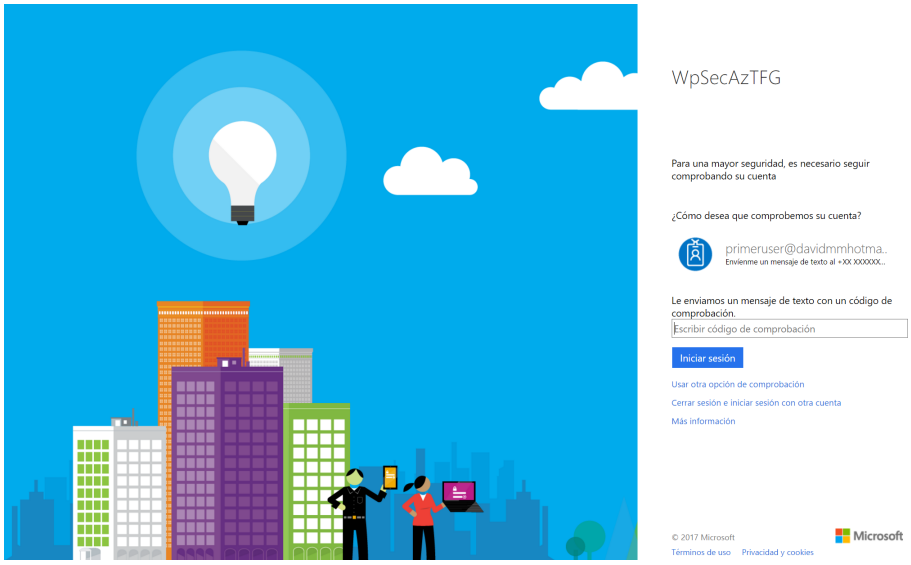


Figura C.7: Inicio Sesión WP Azure

Dicha aplicación está publicada en http://wpsecaztfg.azurewebsites.net/

C.3. Creación de una web ASP con autenticación Single Sing On

En esta sección se va a detallar cómo se crearía una página ASP y se realizará la autenticación de usuarios mediante Azure Active Directory. Se realizará de tal manera que para que un usuario pueda acceder al sistema necesite estar autenticado contra el sistema. ASP es un lenguaje de programación y dado que hay multitud de guías en Internet para crear páginas en ASP únicamente se explicarán los pasos para crear el sitio web y efectuar las configuraciones necesarias para crear un login seguro dejando la plantilla por defecto que nos da ASP al crear el proyecto. Para efectuar estos pasos necesitamos una suscripción Azure y Visual Studio en cualquiera de sus ediciones con ASP para sitios web instalado. Visual Studio tiene una versión gratuita denominada 'Community', la versión utilizada por el autor será la Enterprise 2017, aunque con cualquiera de ellas se puede realizar este escenario. Dicho manual está basado en el que provee Microsoft en `https://technet.microsoft.com/en-us/library/cc771564(v=ws.11).aspx` para la versión de Visual Studio 2013.

Abriremos VS y pulsaremos en 'Nuevo proyecto', seleccionaremos 'ASP WEB application', le daremos un nombre al proyecto y su ubicación en nuestro directorio. Si en este momento u otro se nos pide autenticarnos, deberemos hacerlo con el usuario que tiene la suscripción de Azure, pulsaremos en 'cambiar autenticación' y en esa ventana marcaremos 'Nube: Organización única' y leer datos del directorio. En el cuadro de texto de dominio, si no nos lo sabemos o no nos aparece por defecto, nos dirigiremos al portal de Azure, pestaña Azure Active Directory, nombres de dominio y copiaremos el que nos aparezca. Una vez hecho esto, seleccionaremos que la aplicación será del tipo MVC (Model View Controler) (Figura: Autenticación ASP AAD)

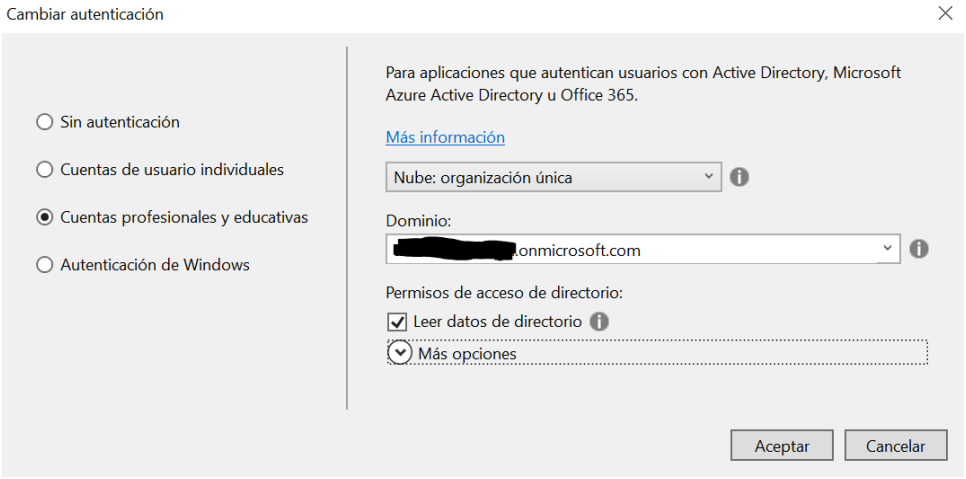


Figura C.8: Autenticación ASP AAD

Esto creará el proyecto de manera local, pero no lo publicará en Azure ni lo publicará en Internet (En versiones anteriores DE vs si se publica por defecto), lo que nos permite modificar el código de la aplicación antes de publicarla (No se hará una demostración de la modificación del código en este documento).

Cuando creamos la aplicación ASP en VS 2017 vemos una ventana con varias opciones: Introducción con ciertos manuales y consejos; Servicios conectados para usar diferentes apis y Publicar para publicar dicha aplicación en Azure. Esta es la opción que deseamos en este momento, así que la utilizaremos, como aún no hemos creado un enlace entre la aplicación y AAD (como hicimos con Wordpress) hemos de crearla, por ello, pulsaremos en nuevo servicio de aplicaciones de Microsoft Azure (En versiones anteriores de VS se crea por defecto).

La pantalla que se mostrará en este momento recordará al lector a la 'Creación Wordpress' ya que deberemos de realizar la misma operación, aunque en esta ocasión ya tendremos creado el servicio de aplicaciones, y como nos albergaba hasta un máximo de cinco aplicaciones podremos seguir utilizándola (Figura Creación servicio de aplicaciones ASP 1).

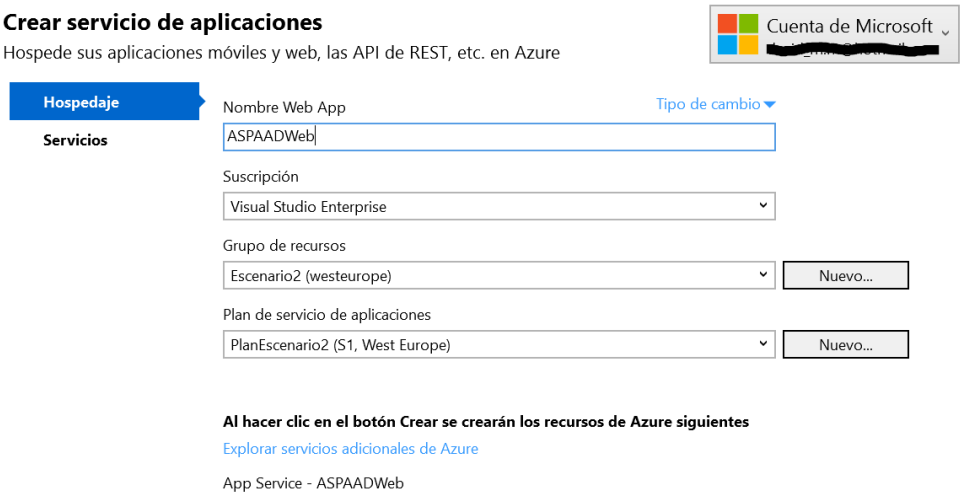


Figura C.9: Creación servicio de aplicaciones ASP 1

Además, deberemos añadir una base de datos que contendrá los datos de la aplicación al igual que hicimos con la aplicación de Wordpress (Figura: Creación servicio de aplicaciones ASP 2).

Figura C.10: Creación servicio de aplicaciones ASP 2

AVISO: Durante la realización de este documento se ha encontrado un error en la librería que utiliza ASP. La cadena de conexión que contiene ASP y que se envía a Azure tiene un error al parsear la cadena si la contraseña del usuario administrador contiene el carácter ;. Se ha reportado a Microsoft, y espero que se repare en una versión próxima, aun así recomiendo no usar estos caracteres en la contraseña del administrador de la base de datos.

Cuando se cree el servicio de aplicaciones, nuestra página web ya estará publicada, pero falta un último paso, que será enlazar la aplicación web en Azure con la URL de nuestra aplicación. Para ello, debemos de acceder a la configuración de la aplicación en Visual Studio y marcaremos la habilitación de la autenticación de la organización. (Este paso debería verse ahorrado porque ya lo hicimos al crear la aplicación, pero hay que repetirlo) (Figura Habilitar autenticación AAD)

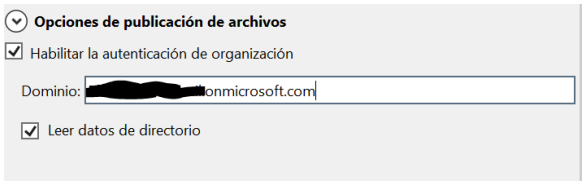


Figura C.11: Habilitar autenticación AAD

Cuando la aplicación termine de publicarse ya podremos acceder con uno de los usuarios que tenemos registrados en nuestro AAD. A esta página web como hemos dicho sólo podremos acceder si nos autenticamos previamente. Todas las páginas del sitio web existentes nos redirigirán a la página de inicio de sesión. Por ejemplo asi accedemos a la página principal de sitio en aspaadweb.azurewebsites.net veremos que se nos redirige a la página de inicio de sesión, al igual que si accedemos a https://aspaadweb.azurewebsites.net/Home/About un página del sitio (Figura: Inicio sesión en ASP).

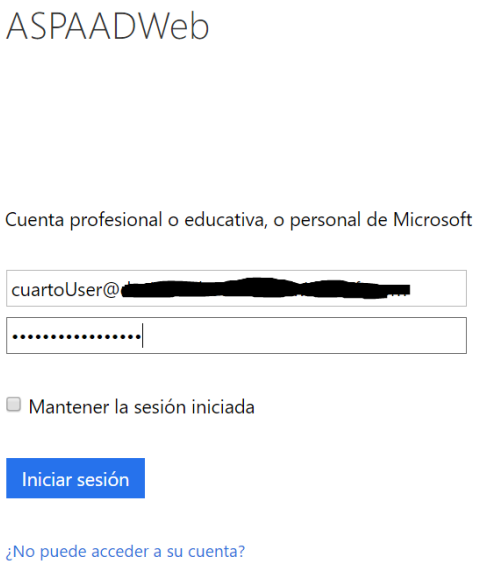


Figura C.12: Inicio sesión en ASP

Además, podemos comprobar cómo este sitio web está protegido por https, lo que significa que todas las peticiones que realicemos contra el servidor estarán codificadas (El certificado lo podemos ver en el siguiente apartado) (Figura: Web ASP).

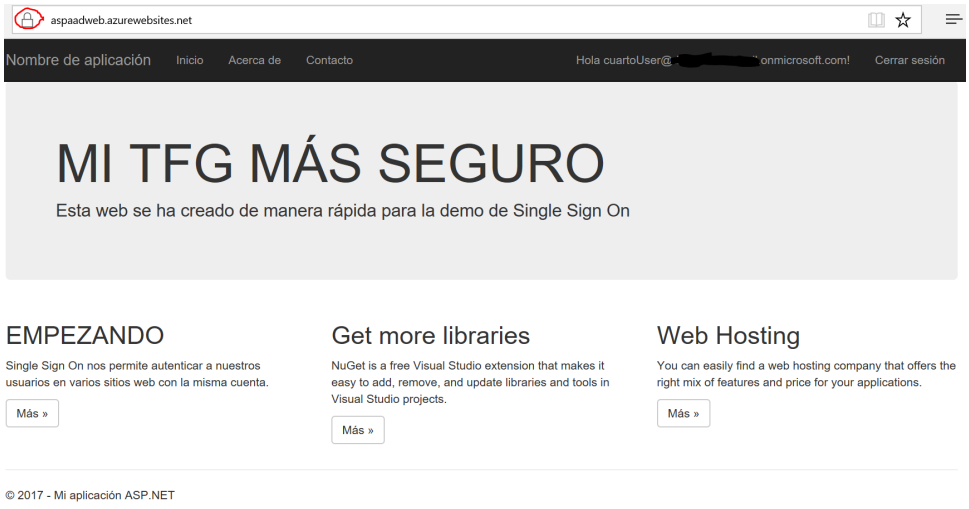


Figura C.13: Web ASP

C.4. Creación de una web que permita registro de usuarios y login a través de aplicaciones externas

Lo primero que hemos de hacer es crear el servicio Azure AD B2C, para ello en el portal de Azure, iremos al panel derecho, más servicios y buscaremos B2C. En vez del típico desplegable de añadir un recurso veremos un enlace marcado como 'Empezar con Azure AD B2C' el cual nos redirigirá a una página web en la que aparecerá un botón para activar el servicio, si le pulsamos nos veremos de nuevo redirigidos al portal de Azure y se nos mostrará la opción

de crear un nuevo inquilino Azure AD B2C o añadir uno existente. Si no tenemos ninguno previamente (caso normal de uso) marcaremos la primera opción. Se nos pedirá el nombre de la organización, un nombre de dominio del tipo 'onmicrosoft.com' y el país de residencia, para crear el servicio pulsaremos en finalizar. Cuando finalice, si hacemos click en el botón superior derecho del portal de azure veremos que tenemos dos directorios. El primero contiene nuestro directorio Azure Active Directory, el segundo el directorio Azure Active Directory B2C. En mi opinión deberían poder administrarse desde el mismo directorio, pero B2C es una tecnología con apenas un año y Azure ha decido hacerlo de este modo. Para empezar no sólo considero que debería poderse administrarse en el mismo directorio por sencillez de uso, sino que al crearnos este nuevo directorio, no tendremos suscripción en el mismo, por lo que para poder consumir las aplicaciones B2C deberemos de asignar una nueva suscripción o enlazar la suscripción de nuestro primer directorio con el nuevo, para ello repetiremos los pasos de creación de directorio B2C hasta el punto en que se nos preguntaba si enlazar un directorio existente y seleccionar dicha opción.

Una vez tenemos creado nuestro directorio estaremos en disposición de crear una aplicación. Una aplicación B2C como las anteriores que hemos realizado se tiene dos componentes, una parte en Azure que se encargará de la autenticación de los usuarios y otra parte de programación, para la cual utilizaremos Visual Studio 2017.

C.4.1. Aplicación en azure

En primer lugar necesitamos una dirección web donde alojar el sitio, para ello como siempre iremos a la pestaña de 'apps services ' y añadiremos una 'web app', alojaremos esta aplicación web en el plan de servicios creado anteriormente, ya que aún tenemos espacio para otras dos páginas web. Ahora tenemos que crear la aplicación B2C en la que se almacenarán los usuarios y sus datos, para ello iremos al directorio B2C, y en las aplicaciones de la izquierda iremos 'Azure AD B2C', en el panel que se nos despliega debemos de seleccionar 'aplicación'; 'nuevo'; se abrirá un nuevo desplegable en el que seleccionaremos en el nombre de la aplicación, marcaremos que se va a usar desde una aplicación web y permitiremos el flujo implícito únicamente si queremos permitir la autenticación desde proveedores externos (Google, facebook...), la dirección de respuesta será la de la página de la aplicación, en mi caso https://b2cwebappdmm.azurewebsites.net/signin-oidc. 'signin-oidc' Corresponde a la redirección que se hace en la aplicación .NET que veremos en el siguiente apartado, pero si no se hace redirección alguna bastaría con la dirección de la aplicación (Figura: Creación aplicación B2C).

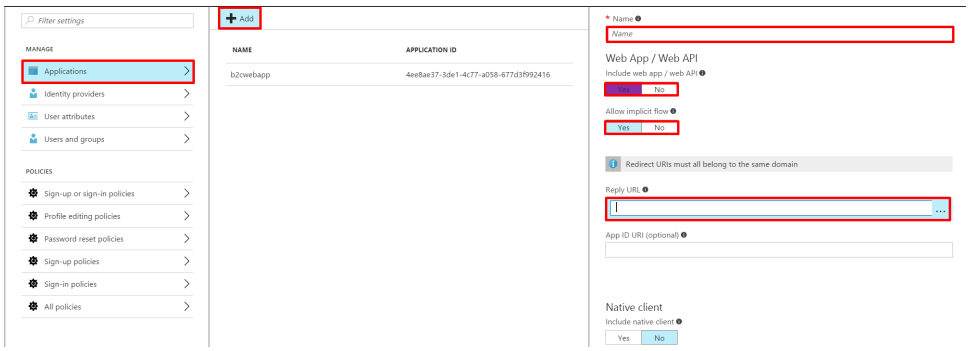


Figura C.14: Creación aplicación B2C

Ahora nos toca decidir los proveedores externos que podrán autenticarse contra esta aplicación, todos aquellos que proveedores que permitan autenticación mediante OpenID son candidatos, podemos encontrar como habilitar autenticación en proveedores como Facebook, Google,

Amazon o linkedin en `https://docs.microsoft.com/es-es/azure/active-directory-b2c/active-directory-b2c-devquickstarts-web-dotnet`. Veremos como habilitar que un usuario con cuenta de facebook se autentique en nuestra aplicación, además en dicha aplicación también podrán autenticarse usuarios con cuentas en google, pero no dedicaré tiempo a explicar cómo dado que se encuentra en la anterior URL.

Habilitando autenticación con cuentas Facebook

En primer lugar, deberemos decir a facebook que tiene que permitir que una aplicación externa utilice usuarios suyos como método de autenticación. Para ello nos dirigiremos a `https://developers.facebook.com/` y nos identificaremos con nuestro usuario de Facebook, sino tenemos uno debemos crearlo, se nos ofrecerá crear una aplicación, de daremos a aceptar (Figura: Creación aplicación Facebook 1).

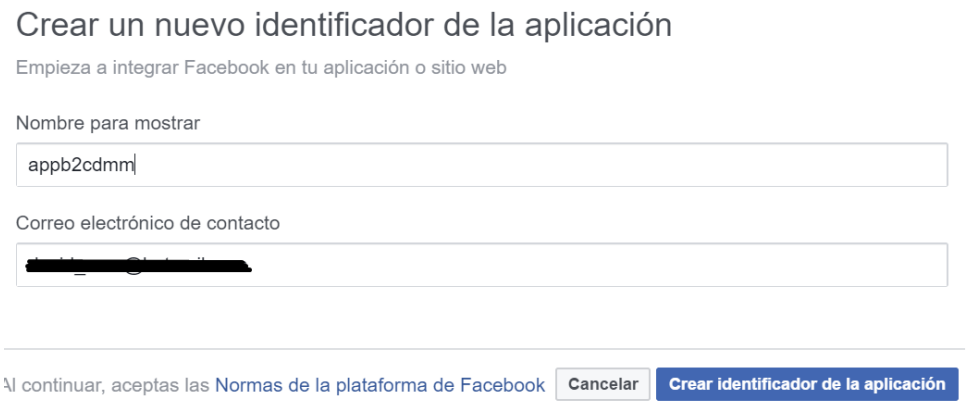


Figura C.15: Creación aplicación Facebook 1

Cuando se haya creado la aplicación deberemos configurarla para que una aplicación web la consuma, para ello iremos a configuración básica y continuación añadir plataforma, seleccionaremos aplicación web e introduciremos la dirección de nuestra web (Figura: Creación aplicación Facebook 2).

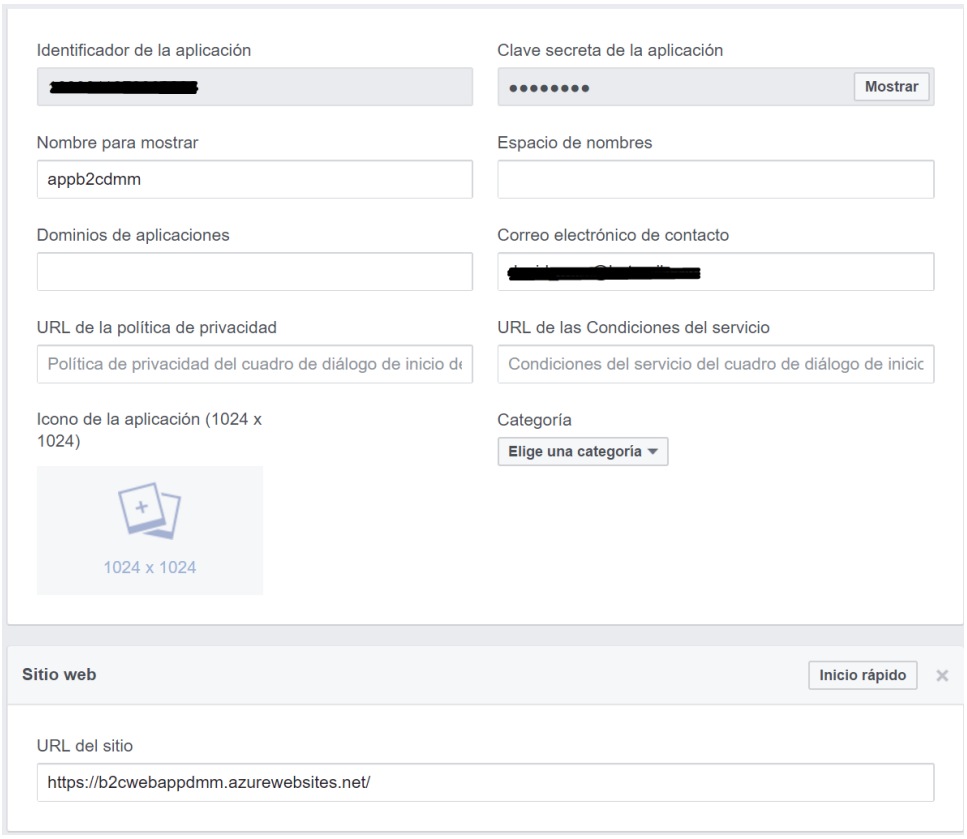


Figura C.16: Creación aplicación Facebook 2

En esa misma pantalla veremos un ID de aplicación y una clave secreta, deberemos copiarlas y no facilitarlas a nadie, ya que cualquier aplicación que use dichas claves podrá utilizar a los usuarios de Facebook. Ahora deberemos añadir un producto del tipo 'Inicio de sesión con Facebook', para ello en el panel izquierdo pulsaremos en 'Añadir producto', 'Inicio de sesión con Facebook' y en el cuadro de texto de la URI de redirección marcaremos `https://login.microsoftonline.com/te/{tenant}/oauth2/authresp` cambiando tenant por el nombre de nuestro directorio. Por último desde la pestaña 'Revisión de la aplicación' la marcaremos como pública para que se pueda consumir desde internet.

El siguiente paso será volver al servicio B2C, pincharemos en proveedores de identidad, añadir. Ahora introduciremos el nombre de la directiva y las dos claves que teníamos copiadas en su campo correspondiente.

Políticas de la aplicación

Ahora vamos a definir los datos que pide la aplicación cuando un usuario se registra en la web, edita su perfil o reestablece su contraseña. Para ello nos dirigimos a la aplicación B2C en el portal de Azure, y en la pestaña 'Politícas' creamos una de registro e inicio de sesión.

- Proveedores de identidad: seleccionamos los proveedores que hayamos creado en el paso anterior y 'Email' para permitir que se registren usuarios sin utilizar proveedores externos.
- Atributos de registro: Serán todos los atributos que queramos que se pida al usuario cuando se registre en nuestra aplicación tales como nombre, ciudad, edad...

- Token: Podemos establecer el tiempo que puede un usuario tener la sesión iniciada en la web.

- Autenticación multi factor: Establecemos si los usuarios requieren de autenticación en dos pasos.

- Personalización de la interfaz: Permite establecer una interfaz distinta a la que viene por defecto cuando los usuarios se autentican.

Crearemos también una política de reestablecimiento de contraseña y edición de perfil seleccionando en 'Atributos de registro' como mucho las mismas opciones que hayamos elegido a la hora de registrar a un usuario.

C.4.2. Código de la aplicación

Para programar la página web se puede utilizar la API graph que provee azure. Dado que ya tienen un ejemplo en `https://github.com/AzureADQuickStarts/B2C-WebApp-OpenIdConnect-DotNet.git` voy a utilizarlo ya que únicamente tendremos que establecer los parámetros de nombre del directorio, ID de la aplicación (En el portal de azure, aplicación B2C, 'Subscription ID') y el nombre de las políticas que hemos creado en el portal de Azure (Figura: Configuración JSON).

Figura C.17: Configuración JSON

Una vez hecho esto, haremos click derecho en el proyecto, publicar y seleccionaremos al aplicación web que creamos al principio de esta subsección

C.4.3. Comprobando el resultado

Si entramos en `https://b2cwebappdmm.azurewebsites.net/` lo primero que vemos si nos fijamos en el explorador es que estamos navegando en un sitio seguro protegido por https el cual podemos examinar y observar que utiliza un algoritmo SHA de 256 bits con clave pública cifrada por RSA de 2048 bits, Aunque Chrome considera que el cifrado está obsoleto. Dicho certificado es el mismo que se emplea en la sección anterior de la web con autenticación SSO aunque no se haya examinado (Figura: Certificado https).

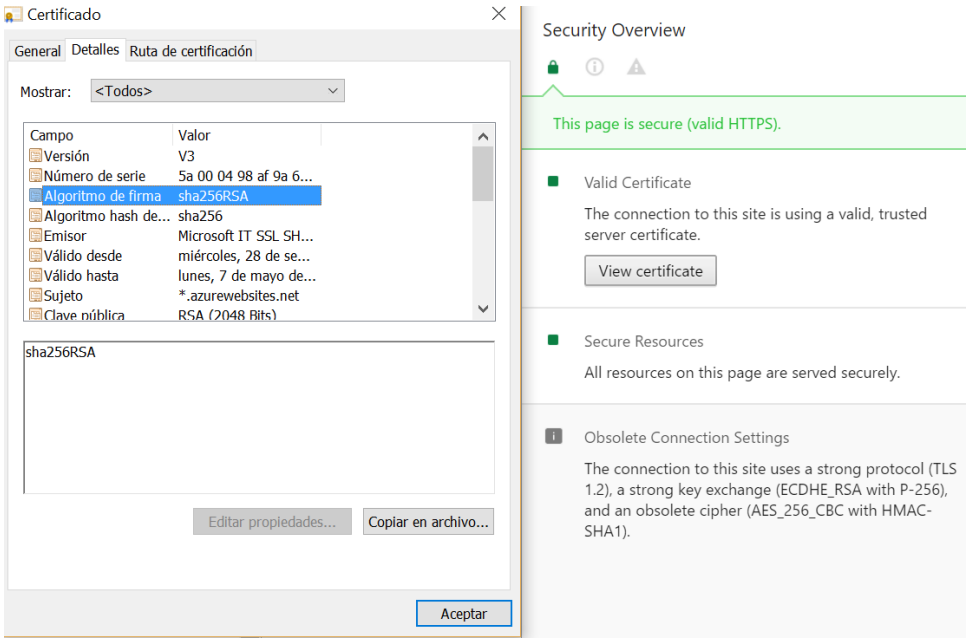


Figura C.18: Certificado https

En dicha página podemos autenticarnos mediante el botón 'Sign in', podremos registrar una nueva cuenta, usar la de facebook o crear una nueva (Figuras: Inicio de sesión, Inicio Facebook, Registro B2C).

Además el administrador desde el portal de Azure podrá ver los usuarios de la aplicación desde la pestaña de usuarios y grupos de la aplicación B2C, todos los datos de los mismos están almacenados en Azure y es Microsoft la encargada de velar por los mismos (Figura: Usuarios B2C).

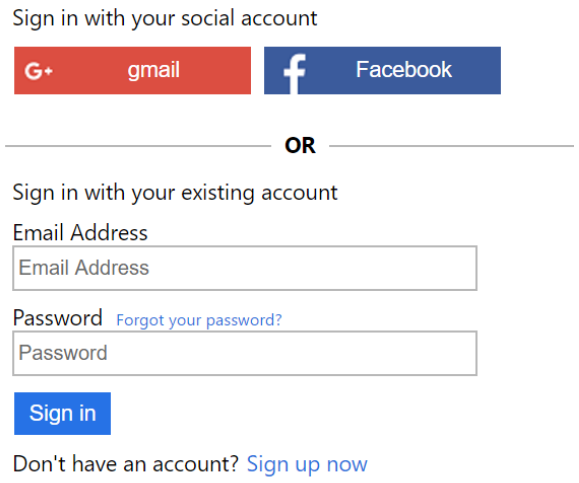


Figura C.19: Inicio de sesión

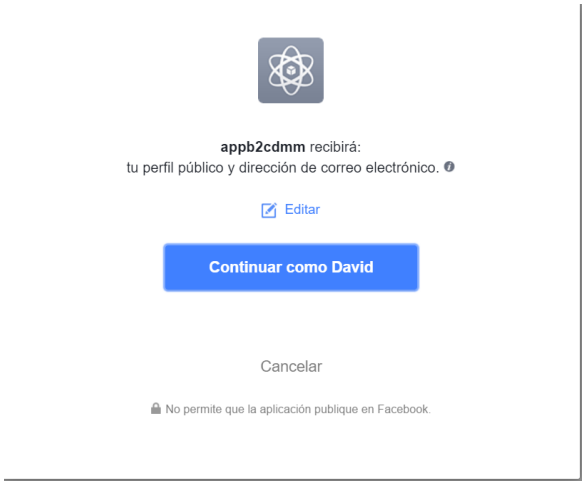


Figura C.20: Inicio Facebook

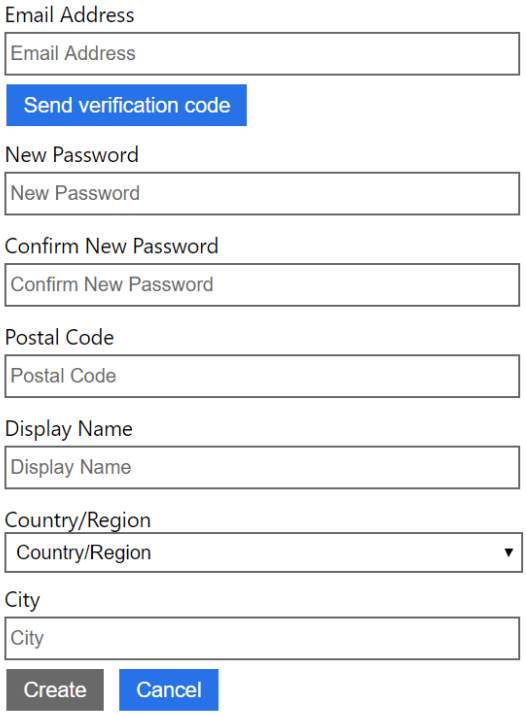


Figura C.21: Registro B2C

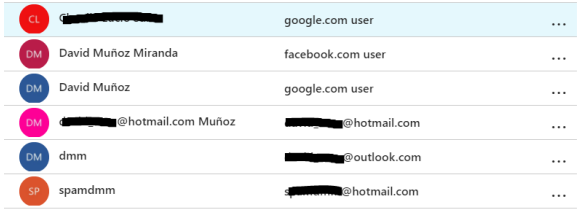


Figura C.22: Usuarios B2C

D

Creación del tercer escenario

Aprovecharemos en este capítulo la aplicación B2C creada en el anexo anterior para mostrar cómo crear una alerta. Para parar nuestra aplicación cuando intuyamos que nos llega un DDOS vamos a necesitas hacer uso de distintas tecnologías que iremos detallando paso por paso

D.1. Cuenta de automatización

Una cuenta de automatización de Azure nos sirve para lanzar scripts de powershell que actuarán sobre los recursos de nuestra cuenta de Azure, a estos scripts se les conoce como 'Runbooks' y desarrollaremos el nuestro en el siguiente apartado. Dichos scripts los podemos publicar en internet para ser consumidos por aplicaciones de forma sencilla, a esto se le conoce como 'Webhook' y también lo veremos.

Para crear una cuenta de automatización, como con cada recurso añadido vamos a pulsar en el panel derecho el icono de 'Más servicios' y en el desplegable buscaremos 'Cuenta de automatización', pulsaremos en añadir, elegiremos un nombre y el grupo de recursos en el que se asocia.

Ahora debemos crear un objeto que guardará nuestras credenciales para ser usado por nuestros scripts, de esta manera no deberemos introducir en plano nuestras credenciales en el script. Para ello dentro de la cuenta de automatización que hemos creado nos dirigiremos a credenciales y añadiremos un nuevo credencial tal y como vemos en la imagen 'Creación de credenciales', se nos pedirá nombre, cuenta y contraseña. Dicha cuenta deberá tener permisos sobre el recurso que se quiera administrar en el script y sólo podrá ser de tipo organizativa (no hotmail o gmail) (Figura: Creación de credenciales).

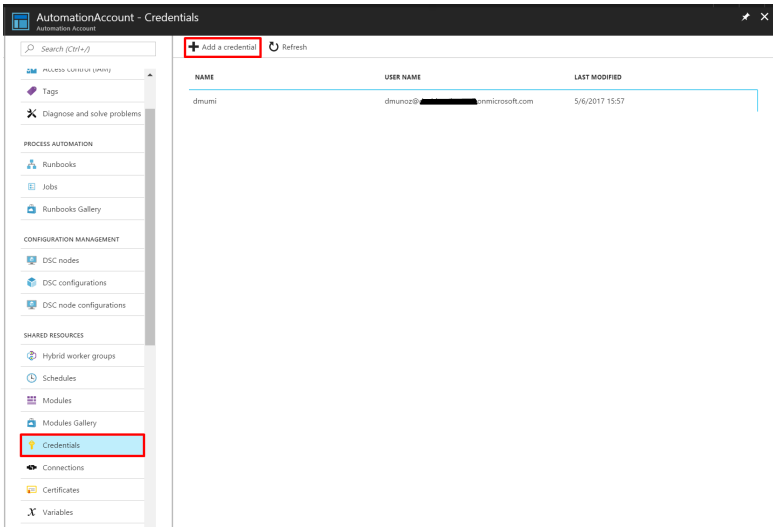


Figura D.1: Creación de credenciales

D.2. Creación del RunBook y el WebHook

Como ya hemos dicho un RunBook es simplemente un script, lo único que dicho script va a estar almacenado en la nube, para crearlo en el panel lateral que se abre en nuestra cuenta de automatización pulsaremos en Runbook y agregaremos uno nuevo, nuestro script deberá parar una aplicación web y con este nos valdrá para ello, podemos verle en la imagen 'Script' (Puede mejorarse dicho script añadiendo comprobaciones pero servirá para nuestro caso). Únicamente deberemos dar el valor del nombre de los credenciales creados en el punto anterior a la variable 'CredentialResource' y el nombre de nuestra aplicación web a la variable 'WebAppName' (Figura Script).

Cuando hayamos configurado el script, si pulsamos en el botón 'Test panel' podemos ejecutarlo para probarlo, si da algún error comprobar el nombre de las credenciales y de la aplicación web. Cuando hayamos comprobado que funcione, pulsaremos en el botón publicar para que se apliquen los cambios.

Ahora, pulsaremos en el botón 'WebHook' para publicarlo en la web, debemos darle un nombre y una fecha de caducidad, la creación se puede ver en la imagen de webhook. Es muy importante copiar la url que nos aparece, ya que será la que consumamos con la alarma y no se volverá a mostrar una vez guardemos (Figura webhook).

D.3. Creación de la alerta

Con el script publicado, seleccionaremos la aplicación que queramos proteger, e iremos a la pestaña de 'Alertas', pincharemos en añadir alerta. Se nos pedirá un nombre para la misma, si se aplicará sobre una métrica o un evento (Evento sería por ejemplo un reinicio del servicio, métricas mediciones como los datos entrantes así que seleccionaremos dicha opción), cuándo se aplica (datos entrantes), evento (condición comparativa con la métrica), activación (tendríamos que medir previamente los datos que recibimos), periodo, correo electrónico al que se nos avisará y dirección del webhook. Como podemos ver en la figura 'Creación de alerta' así se crearía una alerta que nos enviaría un correo cuando se alcance dicha métrica. Un ejemplo de dicho correo lo podemos ver en la figura 'Mensaje de alerta', además podemos comprobar que la aplicación ahora muestra un error 403 y no responde (Figuras Error 403).

```
Workflow stop-webapp
{

    <#
    $CredentialResource es el nombre de los credeciales que se encuentrar en la cuenta de automatizacion
    $WebAppName es el nombre de la $webApp a reiniciar
    #>
    $CredentialResource = "dmumi"
    $WebAppName = "b2cwebappdmm"

    <#
    Recupera información acerca de un recurso de credencial
    https://docs.microsoft.com/es-es/azure/automation/automation-credentials
    #>
    $Cred = Get-AutomationPSCredential -Name $CredentialResource

    <#
    Usa las credenciales en ARM
    https://docs.microsoft.com/es-es/powershell/module/azurerm.profile/add-azurermaccount?view=azurermps-4.0.0
    #>
    Add-AzureRmAccount -Credential $Cred
    <#
    Añade la cuenta de Azure a powershell
    https://docs.microsoft.com/en-us/powershell/module/azure/add-azureaccount?view=azuresmps-4.0.0
    #>
    Add-AzureAccount -Credential $Cred

    <#
    Guarda la pagina de azure
    https://docs.microsoft.com/en-us/powershell/module/azure/get-azurewebsite?view=azuresmps-4.0.0
    #>
    $webApp = Get-AzureWebsite | where-object -FilterScript{$_.name -eq $WebAppName }
    <#
    Detiene la instancia
    https://docs.microsoft.com/en-us/powershell/module/azure/stop-azurewebsite?view=azuresmps-4.0.0
    #>
    Stop-AzureWebsite $webApp.Name
}
```

Figura D.2: Script

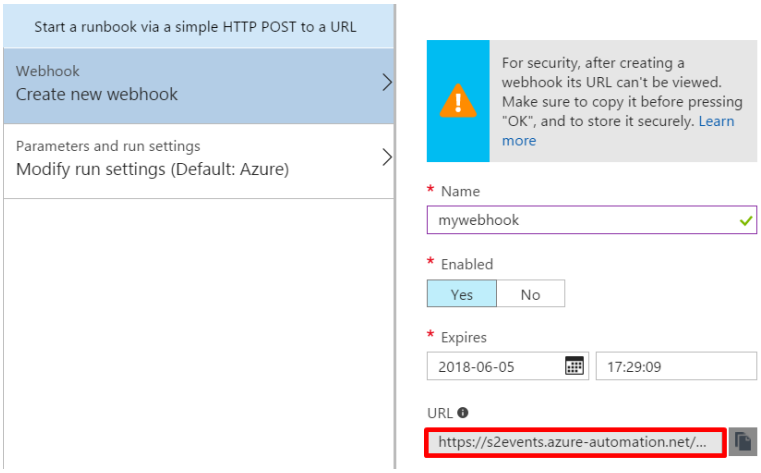


Figura D.3: webhook

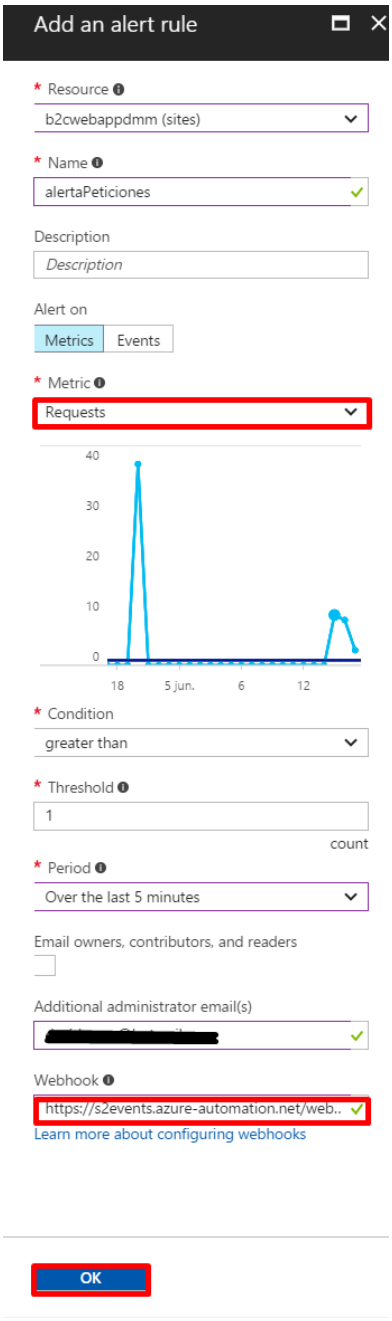


Figura D.4: Creación de alerta

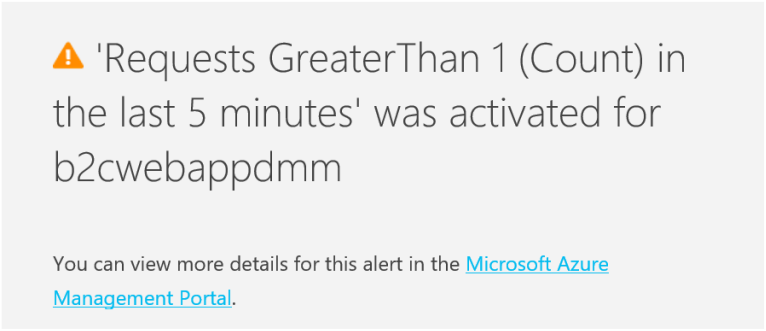


Figura D.5: Mensaje de alerta

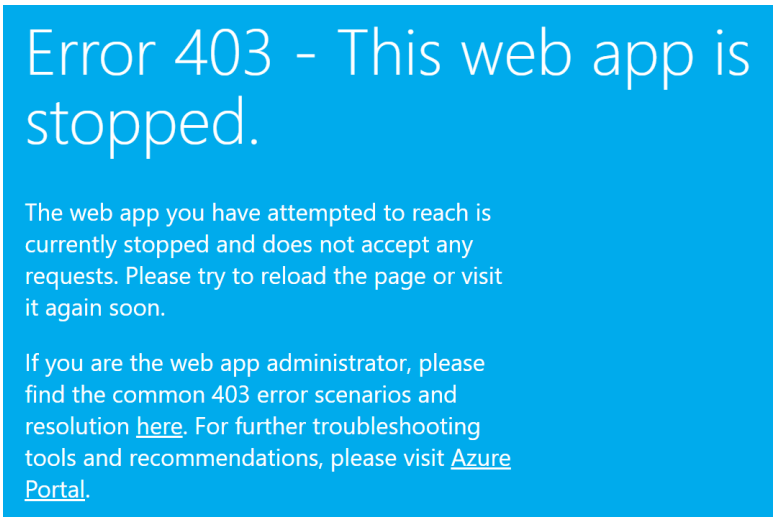


Figura D.6: Error 403

E

Autenticación multi factor en el portal de Azure

Para entrar en el portal de Azure utilizando dos medios distintos hay que seguir pasos sencillos. En primer lugar, en Azure Active Directory debemos de tener registrado al usuario al que se quiere habilitar la autenticación multi-factor, para ello en la sección de Azure Active Directory debemos de ir a usuarios y grupos –> Todos los usuarios. En la pantalla en la que se muestra la lista de usuarios, hay un panel superior en el que debemos pulsar el botón de MultiFactor Authentication. Esta acción nos redirigirá a otra web, en dicha web se nos mostrarán a los usuarios del dominio (Figura: Habilitar MFA).

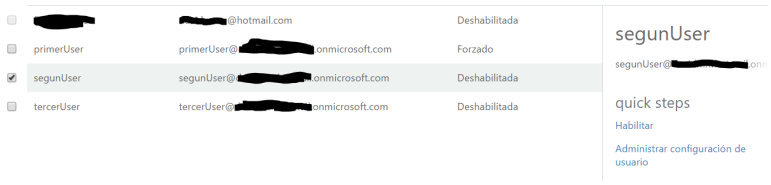


Figura E.1: Habilitar MFA

Seleccionamos el usuario al que queremos habilitar la MFA, pulsamos y pulsamos en habilitar. Con esto el usuario ya podrá entrar al portal de Azure utilizando la autenticación multifactor, dicho usuario deberá configurar cómo se hará este proceso.

La primera vez que dicho usuario accede al portal a través de `portal.azure.com` deberá de configurar el proceso (Figura: Primer Login en el portal).

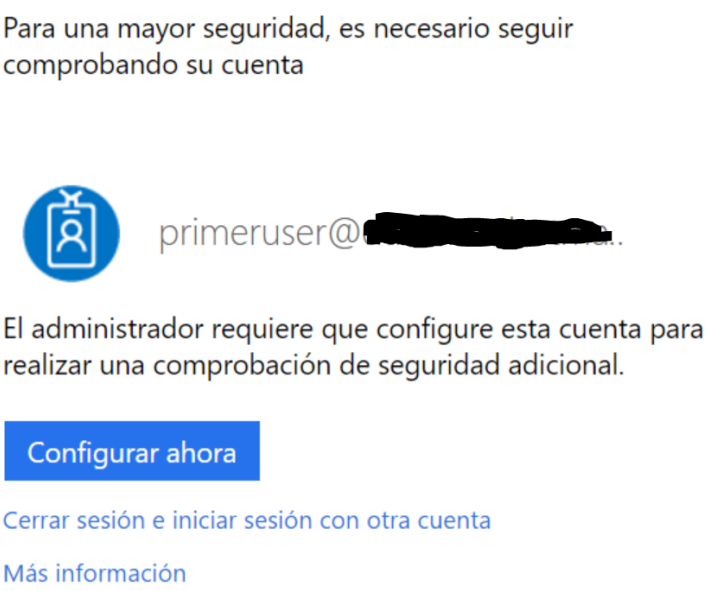


Figura E.2: Primer Login en el portal

A continuación, se le ofrecen las posibilidades, desde un SMS, huella dactilar, aplicación... La única opción que permite la autenticación sin tener que instalar un servidor es la opción móvil, por lo que yo he seleccionado SMS.

En el siguiente paso se pedirá el número de teléfono y se le mandarán un código de activación. A partir de dicho momento cada vez que el usuario intenté autenticarse en el portal, después de insertar su usuario y contraseña se le enviará un código por SMS que deberá de introducir en la página de inicio de sesión. Para deshabilitar dicho proceso, el administrador debe volver a la página donde se habilitaba la MFA y desactivarla para dicho usuario.